READ THIS FIRST - How To Set Up Dell Encryption Key Manager On Your PowerVault™ ML6000 (English) 3

À LIRE EN PREMIER LIEU - Installation de Dell Encryption Key Manager sur votre bibliothèque PowerVault™ ML6000 (French) 10

BITTE ZUERST LESEN - So richten Sie Dell Encryption Key Manager in Ihrem PowerVault™ ML6000 ein (German) 18

LEA ESTO PRIMERO: Cómo instalar Dell Encryption Key Manager en la biblioteca PowerVault™ ML6000 (Spanish) 25

ПРОЧИТАЙТЕ В ПЕРВУЮ ОЧЕРЕДЬ! Установка диспетчера ключей шифрования Dell в библиотеке PowerVault™ ML6000 (Russian) 33

はじめに『PowerVault™ ML6000 に Dell Encryption Key Manager を設定する方法』（Japanese）をお読みください。. 41

이 부분을 먼저 읽으십시오 - PowerVault ™ ML6000 에서 Dell 암호화 키 관리자 설정 방법 (Korean) 48

请先阅读 - 《How To Set Up Dell Encryption Key Manager On Your PowerVault™ ML6000 （如何在 PowerVault™ ML6000 上设置 Dell Encryption Key Manager ）》（Simplified Chinese） 55

請先閱讀 - 如何在 PowerVault™ ML6000 上設定 Dell Encryption Key Manager （Traditional Chinese） 61

May 2010
P/N 6-01856-04

www.dell.com | support.dell.com

Information in this document is subject to change without notice.
© 2010 Dell Inc. All rights reserved. Printed in the U.S.A.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell* and the *DELL* logo are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Les informations contenues dans ce document sont sujettes à modification sans préavis.
© 2010 Dell Inc. Tous droits réservés. Imprimé aux États-Unis.

Toute reproduction de quelque manière que ce soit sans l'autorisation écrite de Dell Inc. est strictement interdite.

Marques utilisées dans ce texte : *Dell* et le logo *DELL* sont des marques de Dell Inc. D'autres marques et noms de marques peuvent être utilisés dans ce document pour se référer aux entités revendiquant les marques et noms de leurs produits respectifs. Dell Inc. dénie tout intérêt propriétaire vis-à-vis des marques et des noms de marques autres que les siens.

Irrtümer und technische Änderungen vorbehalten.
© 2010 Dell Inc. Alle Rechte vorbehalten. Gedruckt in den USA.

Die Reproduktion dieses Dokuments in jeglicher Form ohne schriftliche Genehmigung von Dell Inc. ist streng untersagt.

In diesem Text verwendete Marken: *Dell* und das *DELL*-Logo sind Marken von Dell Inc. Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der jeweiligen Hersteller und Firmen. Dell Inc. lehnt jegliche Besitzrechte an Markenzeichen und Handelsbezeichnungen mit Ausnahme der eigenen ab.

La información contenida en este documento está sujeta a cambios sin previo aviso.
© 2010 Dell Inc. Todos los derechos reservados. Impreso en los EE.UU.

La reproducción de cualquier manera, sea cual sea, sin el permiso por escrito de Dell Inc. está estrictamente prohibida.

Las marcas comerciales que se usan en este texto: *Dell* y el logotipo *DELL* son marcas comerciales de Dell Inc. Es posible que se usen otras marcas comerciales o nombres comerciales en este documento para referirse a las entidades que reclaman la propiedad de las marcas y nombres o a sus productos. Dell Inc. rechaza cualquier interés de propiedad sobre las marcas y nombres comerciales que no sean los suyos.

Информация в данном документе может быть изменена без предварительного уведомления.
© 2010 Dell Inc. Все права защищены. Отпечатано в США.

Воспроизведение данного документа каким бы то ни было способом без письменного разрешения компании Dell Inc. строго запрещено.

Используемые в данном тексте товарные знаки *Dell* и логотип *DELL* являются товарными знаками компании Dell Inc. В настоящем документе могут использоваться другие товарные знаки и наименования для указания соответствующих компаний, зарегистрировавших товарные знаки, и наименований выпускаемых ими изделий. Компания Dell Inc. не претендует на права собственности на какие-либо товарные знаки и наименования, кроме своих собственных.

このマニュアルの内容は予告なしに変更されることがあります。
© 2010 Dell Inc. All rights reserved. Printed in the U.S.A.

Dell Inc. からの書面による許可なしには、いかなる方法においてもこのマニュアルの複写、転載を禁じます。

本書で使用されている商標 : Dell および DELL ロゴは Dell Inc. の商標です。このマニュアルでは、上記以外の商標や会社名が、その商標および商号を主張する事業体またはその製品として使用されている場合があります。これらの商標や会社名は、Dell Inc. に所属しません。

이 문서의 정보는 공지없이 변경될 수 있습니다 .
© 2010 Dell Inc. 모든 권리 소유 . 미국에서 인쇄 .

Dell Inc. 의 서면 승인없이 어떠한 방법으로든 복제하는 것은 절대 금지합니다 .

이 문서에 사용된 상표 : *Dell* 및 *DELL* 로고는 Dell Inc. 의 상표입니다 . 이 문서에 사용된 기타 상표 및 상표명은 상표 및 이름에 대한 권리 소유자 또는 해당 제품을 언급하기 위해 사용되었습니다 . Dell Inc. 은 자사 소유가 아닌 상표 및 상표명에 대한 소유권을 거부합니다

本文挡中的信息如有更改，恕不另行通知。
© 2010 Dell Inc. 版权所有。美国印刷。

未经 Dell Inc. 事先书面同意，严禁 。

本文中使用的商标：*Dell* 和 *DELL* 徽标是 Dell Inc. 的商标。本文档中可能会使用其它商标和商品名称代表声明该商标和名称的实体或其产品。除本公司的商标和商品名称之外，Dell Inc. 对其它公司的商标和商品名称不拥有任何所有权。

本文件中的資訊 若有更動恕不另行通知。
© 2010 Dell Inc. 保留一切權利。於美國列印。

未經由 Dell 的書面允許，禁止以任何形式進行重製動作。

本文中使用的商標：*Dell* 和 *DELL* 標誌是 Dell Inc. 的商標。文件中的其他商標和商標名稱文件中可能會使用其他商標和商標名稱來代表 Dell 的商標和名稱或是產品聲明。 Dell Inc. 對其它公司的商標和商品標籤不擁有任何所有權。

READ THIS FIRST - How To Set Up Dell Encryption Key Manager On Your PowerVault™ ML6000 (English)

About Cautions

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Purpose of This Document

The Dell Encryption Key Manager (EKM) is a centralized key manager application that manages the encryption keys used as part of the IBM LTO-4 and IBM LTO-5 drive-based data encryption process. Library-managed encryption is an optional, licensed feature that must be enabled from the PowerVault ML6000 library in order to begin encrypting data using the LTO-4/LTO-5 tape drive encryption capabilities.

The Dell EKM is an IBM Java software program that assists encryption-enabled tape drives in generating, protecting, storing, and maintaining encryption keys that are used to encrypt information being written to, and decrypt information being read from, tape media. Policy control and keys pass through the library; therefore, encryption is transparent to the applications.

For more information about installing and configuring the EKM server and Dell EKM best practices, please refer to the *Dell PowerVault Encryption Key Manager User's Guide* and the *Dell Encryption Key Manager and Library Managed Encryption Best Practices and FAQ* fact sheet.

NOTE: In order for Dell EKM to work properly, you must upgrade both your library and tape drive firmware to the latest released versions. The latest firmware and installation instructions are available on http://support.dell.com.

Supported Tape Drives and Media

Library managed encryption on the PowerVault ML6000 supports encryption only on LTO-4 and LTO-5 data cartridges using IBM LTO-4 and LTO-5 Fibre Channel and SAS tape drives. ML6000 library managed encryption does not support encryption on other tape drive types or manufacturer brands, even if they are assigned to a partition selected for encryption. Other media types (for example, LTO-3) can be read, but not encrypted, by tape drives enabled for library managed encryption.

Installing the Dell EKM on a Server

You must supply a server or servers on which to install the Dell EKM. When you purchase library managed encryption, you receive a CD which contains the software to install on the server, along with installation instructions and a user's guide. You must set up your EKM server(s) and install your license key before you can set up EKM on your library.

NOTE: Since the Dell PowerVault ML6000 library needs to communicate with the EKM server in real time when reading from or writing to an encryption-enabled tape drive, it is strongly recommended that you use both a primary and secondary EKM server. This way, if the primary server is unavailable at the time the library needs encryption information, the secondary server can handle the request. The Dell PowerVault ML6000 library allows you to use up to two EKM servers for failover/redundancy purposes.

Setting Up Encryption On the Library

Step 1: Installing a License Key

NOTE: Ensure that both your library and tape drive firmware are updated to the latest released versions. The latest firmware and installation instructions are available on www.support.dell.com.

1. Obtain a license key for encryption, following the instructions on the *License Key Certificate* you received.
2. Do one of the following:
   - From the operator panel, select **Setup > Licenses**.
   - From the Web client, select **Setup > License**.
3. Enter the new license key.
4. Click **Apply**.

   A progress window displays, showing time elapsed. When complete, a green **Success** message appears, and the status changes to "Operation Succeeded." Encryption is now listed as a feature on the screen. (If a **Failure** message appears, you may have entered an incorrect license key.)
5. Click **Close**.

Step 2: Configuring Encryption Settings and Key Server Addresses

1. Unload tape cartridges from all encryption-capable tape drives in the library.
2. From the Web client, select **Setup > Encryption > System Configuration**.
3. **Automatic EKM Path Diagnostics**: Enable or disable this feature and set the test interval as desired. You may also specify the number of consecutive missed test intervals required to generate a RAS ticket. For more information, see Automatic EKM Path Diagnostics on page 9.
4. **Secure Sockets Layer (SSL)**: To enable SSL for communication between the library and the EKM key servers, select the **SSL Connection** checkbox. The default is Disabled. If you enable SSL, you must make sure that the **Primary** and **Secondary Key Server Port Numbers** (see below) match the SSL port numbers set on the EKM key servers. The default SSL port number is 443.

NOTE: Keys are always encrypted before being sent from the EKM key server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

5. In the **Primary Key Server IP Address or Host** text box, enter either:
   - The IP address of the primary key server (if DNS is not enabled), or
   - The host name of the primary key server (if DNS is enabled)
6. Enter the port number for the primary key server into the **Primary Key Server Port Number** text box. The default port number is 3801 unless SSL is enabled. If SSL is enabled, the default port number is 443.

NOTE: If you change the port number setting on the library, you must also change the port number on the key server to match or EKM will not work properly.

7. If you are using a secondary key server for failover purposes, enter the IP address or host name of the secondary key server into the **Secondary Key Server IP Address or Host** text box.

NOTE: If you do not plan to use a secondary key server, you may type a zero IP address, 0.0.0.0, into the **Secondary Key Server IP Address or Host** text box, or you may leave the text box blank.

8. If you configured a secondary key server (previous step), enter the port number for the secondary key server into the **Secondary Key Server Port Number** text box. The default port number is 3801 unless SSL is enabled. If SSL is enabled, the default port number is 443.

NOTE: If you are using a secondary key server, then the port numbers for both the primary and secondary key servers must be set to the same value. If they are not, synchronization and failover will not occur.

9. Click **Apply**.

The Progress Window opens. The Progress Window contains information on the action, elapsed time, and status of the operation. Do one of the following:

- If **Success** appears in the Progress Window, the EKM system settings were successfully configured. Click **Close** to close the Progress Window.
- If **Failure** appears in the Progress Window, the EKM system settings were not successfully configured. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

NOTE: If you plan to use different EKM key servers for different partitions, you must also fill in the overrides section of the **Setup** > **Encryption** > **Partition Encryption** screen. See Step 3: Configuring Partition Encryption.

Step 3: Configuring Partition Encryption

Encryption on the Dell PowerVault ML6000 tape library is enabled by partition only. You cannot select individual tape drives for encryption; you must select an entire partition to be encrypted. If you enable a partition for library managed encryption, all library managed encryption-supported tape drives in the partition are enabled for encryption, and all data written to library managed encryption-supported media in the partition is encrypted. Any tape drives not supported by library managed encryption in that partition are not enabled for encryption, and data written to non-supported media is not encrypted.

Data written to encryption-supported and encryption-capable media in library managed encryption-supported tape drives will be encrypted *unless* data was previously written to the media in a non-encrypted format. In order for data to be encrypted, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT).

Configure the partition(s) as follows:

1. From the Web client, select **Setup** > **Encryption** > **Partition Configuration**.

   A list of all your partitions displays, along with a drop-down list displaying the encryption method for each partition.

2. If you want to change the encryption method for a partition, make sure that no tape drives in that partition have cartridges loaded in them. If tape drives have cartridges loaded, you cannot change the encryption method.

3. Select an encryption method from the drop-down list for each partition. (For tape drives that support encryption, the default is **Application Managed**.) The Encryption Method applies to all encryption-capable tape drives and media in that partition.

Encryption Method	Description
Library Managed	**For use with EKM.** Enables encryption support via a connected Dell EKM key server for all encryption-capable tape drives and media assigned to the partition.
Application Managed	**Not for use with EKM.** Allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. The library will NOT communicate with the Dell EKM server on this partition. This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected *unless* you want Dell EKM to manage encryption. **NOTE:** If you want an application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing this type of encryption.
None	Disables encryption on the partition.

www.dell.com | support.dell.com

Unsupported	Means that no tape drives in that partition support encryption. If **Unsupported** is shown, it will be greyed out and you will not be able to change the setting.

4 If you want different partitions to use different EKM key servers, fill in the Library Managed Encryption Server Overrides section as described in this step. The settings in the overrides section supersede the default settings listed in the **Setup > Encryption > System Configuration** screen. (However, the overrides settings do not change the settings listed in the **Setup > Encryption > System Configuration** screen. Those settings are the default configuration settings for any partition that does not use overrides.) Overrides are only available on partitions that have **Library Managed** set as the encryption method.

CAUTION: Only fill in the overrides section if you want different partitions to use different EKM key servers. Otherwise, leave this section alone and allow the values from the Setup > Encryption > System Configuration screen to populate these fields. Once you make any changes to the overrides section, the default values from the Setup > Encryption > System Configuration screen will no longer automatically populate these fields. If you want to return to the default settings after changing the overrides, you must enter them manually.

For each partition that has Library Managed as the encryption method, do the following:

- Type the IP address (if DNS is not enabled) or the host name (if DNS is enabled) of the primary EKM key server in the **Primary Host** text box.
- Type the port number for the primary EKM key server into the **Port** text box. The default port number is 3801, unless SSL is enabled. If SSL is enabled, the default port number is 443.
- If you are using a secondary EKM server, type the address/host name and port number of the secondary EKM key server in the **Secondary Host** and **Port** text boxes.
- Select the **SSL** checkbox if you want to enable Secure Sockets Layer (SSL) for communication between that partition and the EKM servers. The default is Disabled. If you enable SSL, you must make sure that the primary and secondary EKM port numbers in the overrides section match the SSL port numbers set on the EKM servers. The default SSL port number is 443.

NOTE: Keys are always encrypted before being sent from the EKM server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

NOTE: **Restriction on EKM servers used for overrides:** If you are using primary and secondary servers for overrides, the following restriction applies. (If you are not using a secondary server, there are no restrictions.)

Restriction: A given primary server and secondary server must be "paired" and cannot be used in different combinations. For example:
- You can have Server1 as primary and Server2 as secondary for any or all partitions.
- If Server1 is primary and Server2 is secondary on one partition, then in any other partition that you use Server1, Server1 can only be primary and it must be "paired" with Server2 as secondary. You cannot have Server1 as primary and Server3 as secondary on another partition.
- You cannot have Server1 be both primary on PartitionA and secondary on PartitionB.
- You cannot have Server2 be both secondary on PartitionA and primary on PartitionB.

If you use overrides, make sure that you install Dell EKM on all the servers you specify. Then run the Manual EKM Path Diagnostics on each tape drive in every partition configured for EKM to make sure that each tape drive can communicate with and receive keys from the specified EKM key server. For more information, see Using EKM Path Diagnostics on page 7.

5 Click **Apply**.

The Progress Window appears. The Progress Window contains information on the action, elapsed time, and status of the requested operation. Do one of the following:

- If **Success** appears in the Progress Window, the EKM system settings were successfully configured. Click **Close** to close the Progress Window.

- If **Failure** appears in the Progress Window, the EKM system settings were not successfully configured. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

6 Save the library configuration (for instructions, see the *Dell PowerVault ML6000 User's Guide)*.

Step 4: Running EKM Path Diagnostics

Run EKM Path Diagnostics to make sure your tape drives and key servers are connected and running properly. See Using EKM Path Diagnostics on page 7.

Backing Up Keystore Data

Due to the critical nature of the keys in your keystore, it is vital that you back up your keystore data on a non-encrypted device so that you can recover it as needed and be able to read the tapes that were encrypted using those encryption keys associated with that tape drive or library.

Using EKM Path Diagnostics

The EKM Path Diagnostics consists of a series of short tests to validate whether the key servers are running, connected, and able to serve keys as required.

Run the Manual EKM Path Diagnostics any time you change the key server settings or library encryption settings, and when you replace a tape drive. It is recommended that you test each drive that communicates with key manager servers.

The diagnostics consists of the following tests:

NOTE: The tape drive used for the test must be unloaded, ready, and online in order to run any of the tests.

- **Ping** — Verifies the Ethernet communication link between the library and the key servers. If the partition in which the selected tape drive resides uses EKM server overrides, then the override IP addresses are tested (see **Setup > Encryption > Partition Configuration**). If the partition does not use overrides, the default system IP addresses are tested (see **Setup > Encryption > System Configuration**).
- **Drive** — Verifies the tape drive's path in the library (communication from library to tape drive sled and from tape drive sled to tape drive). The tape drive must be unloaded, ready, and online in order to run this test. If this test fails, the Path and Config tests are not performed.
- **Path** — Verifies that EKM services are running on the key servers. This test cannot run if the Drive test fails.
- **Config** — Verifies that the key servers are capable of serving encryption keys. This test cannot run if the Drive test fails.

If any of the tests fail, try the following resolutions and run the test again to make sure it passes:

- **Ping Test Failure** — Verify that the key server host is running and accessible from the network to which the library is connected.
- **Drive Test Failure** — Look for any tape drive RAS tickets and follow the resolution instructions in the ticket.
- **Path Test Failure** — Verify that the key server is actually running and that the port/SSL settings match the library configuration settings.
- **Config Test Failure** — Verify that the EKM server is set up to accept the tape drive you are testing.

There are two ways to perform the diagnostics:

- Manual EKM Path Diagnostics
- Automatic EKM Path Diagnostics

The Manual diagnostics differs from the Automatic diagnostics in the following ways:

- The Manual diagnostics takes affected partitions offline. The Automatic diagnostics does not take partitions offline. It may delay moves to tape drives while they are being tested.
- The Manual EKM Path Diagnostics requires that you select one tape drive to use for the test. Since the test only validates the selected drive, if you want to test the path for each tape drive, you must run the test multiple times (once for each drive). To test all servers, you must run the diagnostics once for each Library Managed Encryption enabled partition (each server pair is connected to a unique partition and tape drive). If the tape drive is not available (it must be unloaded, ready, and online), the Drive, Path, and Config tests are not performed.
- The Automatic EKM Path Diagnostics tests every connected EKM server in turn, and the library selects the tape drive to use for each test. If the selected tape drive is not available (it must be unloaded, ready, and online), then the library tries another tape drive that is connected to the key server until it finds one that is available. If no tape drives connected to a particular key server are available, then that server is skipped and the tests are not performed. If a server is skipped for "X" number of consecutive test intervals (where "X" is configurable on the Web client), the library generates a RAS ticket. If a tape drive remains loaded for a long time, it is possible that it will never be tested. If you want to test a specific tape drive, then you should use the Manual EKM Path Diagnostics. In particular, if you replace a tape drive, run the Manual EKM path diagnostics.

Manual EKM Path Diagnostics

1. Access the EKM Path Diagnostics screen in one of two ways:
   - Enter library Diagnostics (select **Tools > Diagnostics**) and then select **EKM > EKM Path Diagnostics**. Note that entering Diagnostics will log off all other users of the same or lower privileges and take your partitions offline. When you exit Diagnostics, the partitions automatically come back online.
   - Select **Setup > Encryption > System Configuration** or **Setup > Encryption > Partition Configuration** and click the link that says "Click here to run EKM Path Diagnostics." Note that performing this action takes the partition in which the selected tape drive resides offline. When the test completes, the partition automatically comes back online.

   A list of all the tape drives enabled for library-managed encryption is displayed, along with the tape drive status and the partition in which each tape drive resides.
2. Select the tape drive on which you want to perform diagnostics and click **Apply**. The tape drive must be unloaded, ready, and online in order for the test to run.

   A dialog box appears telling you that the selected partition will be taken offline.
3. Click **OK** to start the diagnostics.

   The Progress Window appears. The Progress Window contains information on the action, elapsed time, and status of the requested operation.

   The library performs the diagnostics and reports pass/fail results on each of the tests in the Progress Window.

NOTE: The diagnostics tests may take several minutes to complete.

4. Do one of the following:
   - If **Completed** appears in the Progress Window, the diagnostics were performed (this does not mean that the diagnostics passed, just that the diagnostics were performed). Click **Close** to close the Progress Window.
   - If **Failure** appears in the Progress Window, the diagnostics were not able to be performed. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

Automatic EKM Path Diagnostics

You can enable the library to automatically perform EKM Path Diagnostics at selected intervals. During each interval, the library tests every configured key server. The library generates a RAS ticket if there are problems. By default, this feature is disabled. The default test interval is four hours. It is recommended that you leave Automatic EKM Path Diagnostics disabled, unless network interruptions are a common cause of encryption failures at your site.

CAUTION: Running Automatic EKM Path Diagnostics may cause an increase in RAS tickets if tests are skipped due to tape drives being unavailable for a configurable number of consecutive test intervals. To reduce the occurrences of RAS tickets, you can specify the number of consecutive test intervals required to generate a RAS ticket to a higher number, or you can set the library to never generate a RAS ticket for missed test intervals.

For a list of tests performed, see Using EKM Path Diagnostics on page 7.

To enable Automatic EKM Path Diagnostics:

1. From the Web client, select **Setup > Encryption > System Configuration**.
2. Select the **Automatic EKM Path Diagnostics** check box.
3. Select an interval from the drop-down list.
4. Specify the number of consecutive, missed test intervals required before the library generates a RAS ticket informing you that the test could not be performed within the specified intervals.

Viewing Tape Drive Encryption Settings

You can view the encryption settings in the following ways:

- **System Information Report** — To view encryption information on all key servers, partitions, and tape drives, select **Reports > System Information** from the Web client. For more information, see the *Dell PowerVault ML6000 User's Guide*.
- **Library Configuration Report** — To view the encryption status of a selected tape drive or tape cartridge, select **Reports > Library Configuration** from the Web client and click a tape drive or slot. The encryption status is displayed in a pop-up status window. For more information, see the *Dell PowerVault ML6000 User's Guide*.
- **Partition Encryption** — From the Web client, select **Setup > Encryption > Partition Configuration** to view and change the encryption settings of partitions. See Step 3: Configuring Partition Encryption on page 5 for more details.

www.dell.com | support.dell.com

À LIRE EN PREMIER LIEU - Installation de Dell Encryption Key Manager sur votre bibliothèque PowerVault™ ML6000 (French)

À propos des mises en garde

ATTENTION ! Une MISE EN GARDE indique un risque de dommage matériel ou de perte de données si les instructions ne sont pas respectées.

Objet de ce document

Dell Encryption Key Manager (EKM) est une application gestionnaire de clés centralisée qui gère les clés de cryptage utilisées en tant que partie intégrante du processus de cryptage des données s'articulant autour des lecteurs IBM LTO-4 et IBM LTO-5. Library Managed Encryption (cryptage géré par la bibliothèque) est une fonctionnalité facultative, sous licence, qui doit être activée depuis la bibliothèque PowerVault ML6000 afin de pouvoir crypter des données à l'aide des fonctionnalités de cryptage du lecteur de bande LTO-4/LTO-5.

Dell EKM est un programme logiciel IBM Java qui aide les lecteurs de bande prenant en charge le cryptage à générer, protéger, stocker et gérer les clés de cryptage utilisées pour crypter les informations écrites sur le média de bande et à décrypter les informations lues à partir de celui-ci. Le contrôle de la stratégie et les clés transitent par l'interface ; par conséquent, le cryptage est transparent pour toutes les applications.

Pour plus d'informations sur l'installation et la configuration du serveur EKM et des recommandations sur Dell EKM, reportez-vous aux documents suivants : *Guide d'utilisation de Dell PowerVault Encryption Key Manager*, *Dell Encryption Key Manager et Library Managed Encryption - Recommandations*, et la feuille d'information *Forum Aux Questions*.

REMARQUE : Afin que Dell EKM puisse fonctionner correctement, vous devez mettre à niveau votre bibliothèque et micrologiciel de lecteur de bande avec les dernières versions officielles. Le dernier micrologiciel et les instructions d'installation les plus récentes sont disponibles à l'adresse http://support.dell.com.

Lecteurs de bande et médias pris en charge

Library Managed Encryption sur la bibliothèque PowerVault ML6000 prend uniquement en charge le cryptage sur les cartouches de données LTO-4 et LTO-5 à l'aide des lecteurs de bande IBM LTO-4 et LTO-5 Fibre Channel et SAS. Library Managed Encryption sur ML6000 ne prend pas en charge le cryptage sur d'autres types de lecteur de bande ou d'autres marques de fabricant, même s'ils sont affectés à une partition sélectionnée pour le cryptage. D'autres types de médias (par exemple, LTO-3) peuvent être lus, mais non cryptés, par des lecteurs de bande activés pour Library Managed Encryption.

Installation de Dell EKM sur un serveur

Vous devez disposer d'un ou de plusieurs serveurs sur lesquels installer Dell EKM. Lorsque vous achetez Library Managed Encryption, vous recevez un CD qui contient le logiciel à installer sur le serveur, ainsi que les instructions d'installation et un guide d'utilisation. Vous devez configurer votre ou vos serveurs EKM et installer votre clé de licence pour pouvoir installer EKM sur votre bibliothèque.

REMARQUE : Étant donné que la bibliothèque Dell PowerVault ML6000 doit communiquer avec le serveur EKM en temps réel lors de la lecture ou de l'écriture sur un lecteur de bande prenant en charge le cryptage, il est fortement recommandé d'utiliser deux serveurs EKM, un principal et un secondaire. Ainsi, si le serveur principal n'est pas disponible lorsque la bibliothèque requiert des informations de cryptage, le serveur secondaire est à même de traiter la demande. La bibliothèque Dell PowerVault ML6000 vous permet de configurer jusqu'à deux serveurs EKM pour des raisons de basculement et de redondance.

Configuration du cryptage sur la bibliothèque

Étape 1 : Installation d'une clé de licence

REMARQUE : Assurez-vous de mettre à niveau vos bibliothèque et micrologiciel de lecteur de bande avec les dernières versions officielles. Le dernier micrologiciel et les instructions d'installation les plus récentes sont disponibles à l'adresse www.support.dell.com.

1. Procurez-vous une clé de licence pour le cryptage, en suivant les instructions qui figurent sur le *certificat de clé de licence* que vous avez reçu.
2. Effectuez l'une des actions suivantes :
   - Dans le panneau de commande, sélectionnez **Setup (Configuration) > Licenses (Licences)**.
   - Dans le client Web, sélectionnez **Setup (Configuration) > License (Licence)**.
3. Entrez la nouvelle clé de licence.
4. Cliquez sur **Apply (Appliquer)**.

   Une fenêtre de progression indiquant le temps écoulé s'affiche. Lorsque l'opération est terminée, un message de **réussite** vert apparaît et l'état est défini sur « Operation Succeeded (L'opération a réussi) ». Encryption (Cryptage) est désormais répertorié en tant que fonctionnalité à l'écran. Si un message d'**échec** apparaît, vous avez probablement entré une clé de licence incorrecte.
5. Cliquez sur **Close (Fermer)**.

Étape 2 : Configuration des paramètres de cryptage et des adresses des serveurs de clés

1. Déchargez les cartouches de bande de tous les lecteurs de bande prenant en charge le cryptage dans la bibliothèque.
2. Dans le client Web, sélectionnez **Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système)**.
3. **Automatic EKM Path Diagnostics (Diagnostics de chemin EKM automatiques)** : activez ou désactivez cette fonctionnalité, puis définissez l'intervalle de test désiré. Vous pouvez également spécifier le nombre d'intervalles de test manqués consécutifs avant la génération d'un dossier RAS. Pour plus d'informations, voir Diagnostics de chemin EKM automatiques, page 16.
4. **Secure Sockets Layer (SSL)** : pour activer SSL pour la communication entre la bibliothèque et les serveurs de clés EKM, cochez la case **SSL Connection (Connexion SSL)**. La valeur par défaut est Disabled (Désactivé). Si vous activez SSL, vous devez vous assurer que **Primary Key Server Port Number** (Numéro de port du serveur de clés principal) et **Secondary Key Server Port Number** (Numéro de port du serveur de clés secondaire) correspondent aux numéros de port SSL définis sur les serveurs de clés EKM (voir ci-dessous). Le numéro de port SSL par défaut est 443.

REMARQUE : Les clés sont toujours cryptées avant d'être envoyées du serveur de clés EKM à un lecteur de bande, que le protocole SSL soit ou non activé. L'activation du protocole SSL renforce la sécurité.

5. Dans la zone de texte **Primary Key Server IP Address or Host (Adresse IP ou hôte du serveur de clés principal)**, entrez :
   - soit l'adresse IP du serveur de clés principal (si DNS n'est pas activé) ;
   - soit le nom d'hôte du serveur de clés principal (si DNS est activé).
6. Entrez le numéro de port du serveur de clés principal dans la zone de texte **Primary Key Server Port Number (Numéro de port du serveur de clés principal)**. Sauf si le protocole SSL est activé, le numéro de port par défaut est 3801. Si le protocole SSL est activé, le numéro de port par défaut est 443.

REMARQUE : Si vous modifiez le paramètre du numéro de port sur la bibliothèque, vous devez également modifier le numéro de port sur le serveur de clés en conséquence ; sinon, EKM ne fonctionnera pas correctement.

7. Si vous utilisez un serveur de clés secondaire à des fins de basculement, entrez l'adresse IP ou le nom d'hôte du serveur de clés secondaire dans la zone de texte **Secondary Key Server IP Address or Host (Adresse IP ou hôte du serveur de clés secondaire)**.

REMARQUE : Si vous n'avez pas l'intention d'utiliser un serveur de clés secondaire, vous pouvez taper une adresse IP nulle, 0.0.0.0, dans la zone de texte **Secondary Key Server IP Address or Host (Adresse IP ou hôte du serveur de clés secondaire)** ou ne pas renseigner cette zone de texte.

8 Si vous avez configuré un serveur de clés secondaire (étape précédente), entrez son numéro de port dans la zone de texte **Secondary Key Server Port Number (Numéro de port du serveur de clés secondaire)**. Sauf si le protocole SSL est activé, le numéro de port par défaut est 3801. Si le protocole SSL est activé, le numéro de port par défaut est 443.

REMARQUE : Si vous utilisez un serveur de clés secondaire, les numéros de port des serveurs de clés principal et secondaire doivent avoir la même valeur. Sinon, la synchronisation et le basculement n'auront pas lieu.

9 Cliquez sur **Apply (Appliquer)**.

La fenêtre de progression s'ouvre. La fenêtre de progression contient des informations sur l'action, le temps écoulé et l'état de l'opération. Effectuez l'une des actions suivantes :

- Si un message de **réussite** apparaît dans la fenêtre de progression, cela signifie que les paramètres du système EKM ont bien été configurés. Cliquez sur **Close (Fermer)** pour fermer la fenêtre de progression.
- Si un message d'**échec** apparaît dans la fenêtre de progression, cela signifie que les paramètres du système EKM n'ont pas pu être configurés. Suivez les instructions répertoriées dans la fenêtre de progression pour résoudre les problèmes survenus au cours de l'opération.

REMARQUE : Si vous projetez d'utiliser différents serveurs de clés EKM pour différentes partitions, vous devez également renseigner la section Overrides (Priorités) de l'écran **Setup (Configuration) > Encryption (Cryptage) > Partition Encryption (Cryptage des partitions)**. Voir Étape 3 : Configuration du cryptage de la partition.

Étape 3 : Configuration du cryptage de la partition

Sur la bandothèque Dell PowerVault ML6000, le cryptage est activé par partition uniquement. Vous ne pouvez pas sélectionner de lecteurs de bande individuels pour le cryptage ; vous devez sélectionner une partition entière à crypter. Si vous activez une partition pour Library Managed Encryption, tous les lecteurs de bande pris en charge par Library Managed Encryption dans cette partition sont activés pour le cryptage, et toutes les données écrites sur des médias pris en charge par Library Managed Encryption dans la partition sont cryptées. Tout lecteur de bande non pris en charge par Library Managed Encryption dans cette partition n'est pas activé pour le cryptage, et les données écrites sur des médias non pris en charge ne sont pas cryptées.

Les données écrites sur les médias pris en charge par le cryptage et prenant en charge le cryptage dans les lecteurs de bande pris en charge par Library Managed Encryption seront cryptées, *sauf* si les données ont été écrites au préalable sur le média dans un format non crypté. Pour que les données soient cryptées, le média doit être vierge ou avoir été gravé par l'intermédiaire de Library Managed Encryption lors de la première opération d'écriture au début de bande.

Configurez la ou les partitions comme suit :

1 Dans le client Web, sélectionnez **Setup (Configuration) > Encryption (Cryptage) > Partition Configuration (Configuration des partitions)**.

Une liste de toutes vos partitions s'affiche, avec une liste déroulante affichant la méthode de cryptage pour chaque partition.

2 Si vous souhaitez modifier la méthode de cryptage pour une partition, vérifiez qu'aucun lecteur de bande de cette partition ne comporte de cartouche. Dans le cas contraire, vous ne pourrez pas modifier la méthode de cryptage.

3 Sélectionnez une méthode de cryptage dans la liste déroulante pour chaque partition. (Pour les lecteurs de bande prenant en charge le cryptage, la méthode par défaut est **Application Managed (Géré par l'application)**. La méthode de cryptage s'applique à tous les lecteurs de bande et les médias prenant en charge le cryptage dans cette partition.

Méthode de cryptage	Description
Library Managed (Géré par la bibliothèque)	**À utiliser avec EKM.** Active la prise en charge du cryptage par le biais d'un serveur de clés Dell EKM connecté pour tous les lecteurs de bande prenant en charge le cryptage et les médias attribués à la partition.

Application Managed (Géré par l'application)	**À ne pas utiliser avec EKM.** Permet à une application de sauvegarde externe de fournir la prise en charge du cryptage à tous les lecteurs de bande et les médias de la partition prenant en charge le cryptage. La bibliothèque NE communiquera PAS avec le serveur Dell EKM sur cette partition. Il s'agit du paramètre par défaut si vous disposez de lecteurs de bande prenant en charge le cryptage dans la partition. Cette option doit rester sélectionnée, *excepté* si vous souhaitez que Dell EKM prenne en charge le cryptage. **REMARQUE :** Si vous voulez que le cryptage soit géré par une application, vous devez configurer spécialement cette dernière à cet effet. La bibliothèque ne participera pas à l'exécution de ce type de cryptage.
None (Aucun)	Désactive le cryptage sur la partition.
Unsupported (Non pris en charge)	Signifie qu'aucun lecteur de bande de cette partition ne prend en charge le cryptage. Si **Unsupported (Non pris en charge)** s'affiche, il sera grisé et vous ne pourrez pas modifier le paramètre.

4 Si vous souhaitez que différentes partitions utilisent des serveurs de clés EKM différents, renseignez la section Library Managed Encryption Server Overrides (Priorités des serveurs de cryptage gérés par la bibliothèque) comme décrit dans cette étape. Les paramètres de la section Overrides (Priorités) remplacent les paramètres par défaut répertoriés à l'écran **Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système)**. Les paramètres de la section Overrides (Priorités) ne modifient toutefois pas les paramètres indiqués dans l'écran **Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système)**. Ces paramètres sont les paramètres de configuration par défaut de toutes les partitions qui n'utilisent pas de priorités. Les priorités sont uniquement disponibles sur les partitions dont la méthode de cryptage est **Library Managed (Géré par la bibliothèque)**.

ATTENTION ! Renseignez la section Overrides (Priorités) uniquement si vous souhaitez que des partitions différentes utilisent des serveurs de clés EKM différents. Sinon, laissez cette section inchangée et renseignez ces champs avec les valeurs de l'écran Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système). Lorsque vous avez terminé de modifier la section Overrides (Priorités), les valeurs par défaut de l'écran Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système) ne renseignent plus automatiquement ces champs. Si vous souhaitez revenir aux paramètres par défaut après avoir modifié les priorités, vous devez les saisir manuellement.

Procédez comme suit pour chaque partition dont la méthode de cryptage est Library Managed (Géré par la bibliothèque) :

- Tapez l'adresse IP (si DNS n'est pas activé) ou le nom de l'hôte (si DNS est activé) du serveur de clés EKM principal dans la zone de texte **Primary Host (Hôte principal)**.
- Tapez le numéro de port du serveur de clés EKM principal dans la zone de texte **Port**. Sauf si le protocole SSL est activé, le numéro de port par défaut est 3801. Si le protocole SSL est activé, le numéro de port par défaut est 443.
- Si vous utilisez un serveur EKM secondaire, tapez l'adresse ou le nom de l'hôte et le numéro de port du serveur de clés EKM secondaire dans les zones de texte **Secondary Host** (Hôte secondaire) et **Port**.
- Cochez la case **SSL** si vous souhaitez activer le protocole Secure Sockets Layer (SSL) pour établir une communication entre cette partition et les serveurs EKM. La valeur par défaut est Disabled (Désactivé). Si vous activez le protocole SSL, vous devez vérifier que les numéros des ports EKM principal et secondaire dans la section Overrides (Priorités) correspondent aux numéros de ports SSL définis sur les serveurs EKM. Le numéro de port SSL par défaut est 443.

REMARQUE : Les clés sont toujours cryptées avant d'être envoyées du serveur EKM à un lecteur de bande, que le protocole SSL soit ou non activé. L'activation du protocole SSL renforce la sécurité.

REMARQUE : Restrictions de l'utilisation des serveurs EKM pour les priorités : si vous utilisez des serveurs principaux et secondaires pour les priorités, les restrictions suivantes s'appliquent. (Si vous n'utilisez pas de serveur secondaire, il n'y a pas de restrictions.)

Restriction : un serveur principal et un serveur secondaire donnés doivent être « couplés » et ne peuvent pas être utilisés dans des combinaisons différentes. Par exemple :
• Vous pouvez avoir Serveur1 comme serveur principal et Serveur2 comme serveur secondaire pour une ou toutes les partitions.

www.dell.com | support.dell.com

• Si Server1 est principal et Serveur2 est secondaire sur une partition, alors dans d'autres partitions où vous utilisez Serveur1, Serveur1 est uniquement le serveur principal et doit rester « couplé » avec Serveur2 comme serveur secondaire. Vous ne pouvez pas avoir Serveur1 comme serveur principal et Serveur3 comme serveur secondaire sur une autre partition.
• Vous ne pouvez pas avoir Serveur1 comme serveur principal sur PartitionA et comme serveur secondaire sur PartitionB.
• Vous ne pouvez pas avoir Serveur2 comme serveur secondaire sur PartitionA et comme serveur principal sur PartitionB.

Si vous configurez des priorités, installez bien Dell EKM sur tous les serveurs que vous spécifiez. Exécutez ensuite les diagnostics de chemin EKM manuels sur chaque lecteur de bande de chaque partition configurée pour EKM afin de vous assurer que chaque lecteur de bande peut communiquer avec le serveur de clés EKM spécifié et en recevoir des clés. Pour plus d'informations, voir Utilisation de EKM Path Diagnostics (Diagnostics de chemin EKM), page 14.

5 Cliquez sur **Apply (Appliquer)**.

La fenêtre de progression apparaît. La fenêtre de progression contient des informations sur l'action, le temps écoulé et l'état de l'opération demandée. Effectuez l'une des actions suivantes :

- Si un message de **réussite** apparaît dans la fenêtre de progression, cela signifie que les paramètres du système EKM ont bien été configurés. Cliquez sur **Close (Fermer)** pour fermer la fenêtre de progression.
- Si un message d'**échec** apparaît dans la fenêtre de progression, cela signifie que les paramètres du système EKM n'ont pas pu être configurés. Suivez les instructions répertoriées dans la fenêtre de progression pour résoudre les problèmes survenus au cours de l'opération.

6 Enregistrez la configuration de la bibliothèque (pour obtenir des instructions, consultez le *Guide d'utilisation de Dell PowerVault ML6000)*.

Étape 4 : Exécution de EKM Path Diagnostics (Diagnostics de chemin EKM)

Exécutez EKM Path Diagnostics pour vous assurer que vos lecteurs de bande et serveurs de clés sont connectés et fonctionnent correctement. Voir Utilisation de EKM Path Diagnostics (Diagnostics de chemin EKM), page 14.

Sauvegarde des données de l'espace de stockage des clés

En raison de la nature critique des clés présentes dans votre espace de stockage de clés, il est primordial que vous sauvegardiez vos données incluses dans l'espace de stockage de clés sur un périphérique non crypté de sorte que vous puissiez le récupérer en cas de besoin et lire les bandes cryptées à l'aide des clés de cryptage associées à ce lecteur de bande ou à la bibliothèque.

Utilisation de EKM Path Diagnostics (Diagnostics de chemin EKM)

Les diagnostics de chemin EKM consistent en une série de tests courts destinés à vérifier si les serveurs de clés sont en cours d'exécution, connectés et en mesure de fournir des clés en fonction des besoins.

Exécutez les diagnostics de chemin EKM manuels chaque fois que vous modifiez les paramètres du serveur de clés ou les paramètres de cryptage de la bibliothèque, et lorsque vous remplacez un lecteur de bande. Il est recommandé de tester chaque lecteur qui communique avec les serveurs de gestion des clés.

Les diagnostics comprennent les tests suivants :

REMARQUE : Le lecteur de bande utilisé pour le test doit être déchargé, prêt et en ligne pour que les tests puissent être exécutés.

- **Ping** : vérifie la liaison de communication Ethernet entre la bibliothèque et les serveurs de clés. Si la partition dans laquelle réside le lecteur de bande sélectionné utilise des priorités de serveurs EKM, les adresses IP de ces derniers sont alors testées (voir **Setup (Configuration) > Encryption (Cryptage) > Partition Configuration (Configuration des partitions)**). Si la partition n'utilise pas de priorités, les adresses IP par défaut du système sont testées (voir **Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système)**).

- **Drive (Lecteur)** : vérifie le chemin du lecteur de bande dans la bibliothèque (les communications entre la bibliothèque et le chariot du lecteur de bande et entre le chariot du lecteur de bande et le lecteur de bande). Le lecteur de bande doit être déchargé, prêt et en ligne pour que ce test puisse être exécuté. Si ce test échoue, les tests Path et Config ne sont pas effectués.
- **Path (Chemin)** : vérifie que les services EKM sont en cours d'exécution sur les serveurs de clés. Ce test ne peut pas être exécuté si le test Drive échoue.
- **Config** : vérifie que les serveurs de clés sont en mesure de fournir des clés de cryptage. Ce test ne peut pas être exécuté si le test Drive échoue.

Si l'un des tests échoue, essayez les solutions ci-dessous et relancez le test pour vérifier qu'il s'exécute complètement :

- **Ping Test Failure (Échec du test Ping)** : vérifiez que l'hôte du serveur de clés s'exécute et qu'il est accessible depuis le réseau auquel la bibliothèque est connectée.
- **Drive Test Failure (Échec du test Drive)** : recherchez les dossiers RAS du lecteur de bande et suivez les instructions données dans le dossier pour résoudre cet échec.
- **Path Test Failure (Échec du test Path)** : vérifiez que le serveur de clés s'exécute vraiment et que les paramètres du port/SSL correspondent aux paramètres de configuration de la bibliothèque.
- **Config Test Failure (Échec du test Config)** : vérifiez que le serveur EKM est configuré pour accepter le lecteur de bande que vous testez.

Vous pouvez effectuer les diagnostics de deux façons :

- Diagnostics de chemin EKM manuels
- Diagnostics de chemin EKM automatiques

Les différences entre les diagnostics manuels et les diagnostics automatiques sont les suivantes :

- Les diagnostics manuels mettent les partitions affectées hors ligne. Les diagnostics automatiques ne mettent pas les partitions hors ligne. Ils peuvent retarder les déplacements vers les lecteurs de bande lorsqu'ils sont testés.
- Les diagnostics manuels exigent que vous sélectionniez un lecteur de bande pour le test. Étant donné que le test valide uniquement le lecteur sélectionné, si vous voulez tester le chemin pour chaque lecteur de bande, vous devez exécuter le test à plusieurs reprises (une fois pour chaque lecteur). Pour tester tous les serveurs, vous devez exécuter les diagnostics une fois pour chaque partition activée pour Library Managed Encryption (chaque paire de serveurs est connectée à une partition et à un lecteur de bande uniques). En outre, si le lecteur de bande n'est pas disponible (il doit être déchargé, prêt et en ligne), les tests Drive, Path et Config ne sont pas effectués.
- Les diagnostics automatiques testent chaque serveur EKM connecté l'un après l'autre, et la bibliothèque sélectionne le lecteur de bande à utiliser pour chaque test. Si le lecteur de bande sélectionné n'est pas disponible (il doit être déchargé, prêt et en ligne), la bibliothèque sélectionne alors un autre lecteur de bande connecté au serveur de clés jusqu'à ce qu'elle en trouve un de disponible. Si aucun lecteur de bande connecté à un serveur de clés particulier n'est disponible, ce serveur est ignoré et les tests ne sont pas effectués. Si un serveur est ignoré après « X » intervalles de test consécutifs (où « X » est configurable sur le client Web), la bibliothèque génère un dossier RAS. Si un lecteur de bande reste chargé pendant une longue période de temps, il est possible qu'il ne soit jamais testé. Si vous voulez tester un lecteur de bande spécifique, utilisez les diagnostics de chemin EKM manuels. En particulier, si vous remplacez un lecteur de bande, exécutez les diagnostics de chemin EKM manuels.

Diagnostics de chemin EKM manuels

1. Accédez à l'écran EKM Path Diagnostics (Diagnostics de chemin EKM) de l'une des deux manières suivantes :
   - Accédez aux diagnostics de bibliothèque (**Tools (Outils) > Diagnostics**), puis sélectionnez **EKM > EKM Path Diagnostics (Diagnostics de chemin EKM)**. Notez que l'accès aux diagnostics déconnectera tous les autres utilisateurs avec les mêmes privilèges ou privilèges inférieurs et mettra vos partitions hors ligne. Lorsque vous quittez les diagnostics, les partitions sont remises automatiquement en ligne.
   - Sélectionnez **Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système)** ou **Setup (Configuration) > Encryption (Cryptage) > Partition Configuration (Configuration des partitions)**, puis cliquez sur le lien qui indique « Click here to run

www.dell.com | support.dell.com

EKM Path Diagnostics » (Cliquez ici pour exécuter les diagnostics de chemin EKM). Notez que cette action met la partition dans laquelle le lecteur de bande sélectionné réside hors ligne. Lorsque le test est terminé, la partition revient automatiquement en ligne.

Une liste de tous les lecteurs de bande activés pour le cryptage géré par la bibliothèque est affichée avec l'état du lecteur de bande et la partition dans laquelle réside chaque lecteur de bande.

2. Sélectionnez le lecteur de bande sur lequel vous souhaitez exécuter les diagnostics et cliquez sur **Apply (Appliquer)**. Le lecteur de bande doit être déchargé, prêt et en ligne pour que le test puisse être exécuté.

   Une boîte de dialogue vous indique alors que la partition sélectionnée sera mise hors ligne.

3. Cliquez sur **OK** pour lancer les diagnostics.

   La fenêtre de progression apparaît. La fenêtre de progression contient des informations sur l'action, le temps écoulé et l'état de l'opération demandée.

   La bibliothèque exécute les diagnostics et communique les résultats (réussite ou échec) de chacun des tests dans la fenêtre de progression.

REMARQUE : Les tests de diagnostic peuvent durer plusieurs minutes.

4. Effectuez l'une des actions suivantes :
   - Si **Completed (Terminé)** apparaît dans la fenêtre de progression, les diagnostics ont été exécutés (ceci ne signifie pas pour autant qu'ils ont réussi, mais simplement qu'ils ont été effectués). Cliquez sur **Close (Fermer)** pour fermer la fenêtre de progression.
   - Si **Failure (Échec)** apparaît dans la fenêtre de progression, les diagnostics n'ont pas pu être effectués. Suivez les instructions répertoriées dans la fenêtre de progression pour résoudre les problèmes survenus au cours de l'opération.

Diagnostics de chemin EKM automatiques

Vous pouvez configurer la bibliothèque de manière à effectuer automatiquement les diagnostics de chemin EKM à intervalles sélectionnés. Au cours de chaque intervalle, la bibliothèque teste chaque serveur de clés configuré. La bibliothèque génère un dossier RAS s'il y a des problèmes. Par défaut, cette fonctionnalité est désactivée. L'intervalle de test par défaut est de quatre heures. Il est recommandé de laisser les diagnostics de chemin EKM automatiques désactivés, sauf si des interruptions du réseau entraînent fréquemment des échecs de cryptage sur votre lieu de travail.

ATTENTION ! L'exécution des diagnostics de chemin EKM automatiques peut provoquer une augmentation des dossiers RAS si les tests sont ignorés en raison de l'indisponibilité des lecteurs de bande pendant un nombre configurable d'intervalles de test consécutifs. Pour réduire les occurrences des dossiers RAS, vous pouvez spécifier un nombre plus élevé d'intervalles de test consécutifs avant la génération d'un dossier RAS, ou vous pouvez configurer la bibliothèque de manière à ce qu'elle ne génère jamais de dossier RAS en cas d'intervalles de test manqués.

Pour obtenir la liste des tests effectués, voir Utilisation de EKM Path Diagnostics (Diagnostics de chemin EKM), page 14.

Pour activer les diagnostics de chemin EKM automatiques :

1. Dans le client Web, sélectionnez **Setup (Configuration) > Encryption (Cryptage) > System Configuration (Configuration système)**.
2. Cochez la case **Automatic EKM Path Diagnostics (Diagnostics de chemin EKM automatiques)**.
3. Sélectionnez un intervalle de test dans la liste déroulante.
4. Spécifiez le nombre d'intervalles de test manqués consécutifs avant que la bibliothèque ne génère un dossier RAS vous informant que le test ne peut pas être effectué dans les intervalles spécifiés.

Affichage des paramètres de cryptage du lecteur de bande

Vous pouvez afficher les paramètres de cryptage des manières suivantes :

- **System Information Report (Rapport d'informations système)** : pour afficher des informations de cryptage sur tous les serveurs de clés, les partitions et les lecteurs de bande, sélectionnez **Reports (Rapports) > System Information (Informations système)** dans le client Web. Pour plus d'informations, voir le *Guide d'utilisation de Dell PowerVault ML6000*.

- **Library Configuration Report (Rapport de configuration de bibliothèque)** : pour afficher l'état de cryptage d'un lecteur de bande ou d'une cartouche de bande sélectionné, sélectionnez **Reports (Rapports) > Library Configuration (Configuration de bibliothèque)** dans le client Web, puis cliquez sur un lecteur de bande ou sur un logement. L'état du cryptage s'affiche dans une fenêtre d'état contextuelle. Pour plus d'informations, voir le *Guide d'utilisation de Dell PowerVault ML6000*.
- **Partition Encryption (Cryptage des partitions)** : dans le client Web, sélectionnez **Setup (Configuration) > Encryption (Cryptage) > Partition Configuration (Configuration des partitions)** pour afficher et modifier les paramètres de cryptage des partitions. Pour plus d'informations, voir Étape 3 : Configuration du cryptage de la partition, page 12.

BITTE ZUERST LESEN - So richten Sie Dell Encryption Key Manager in Ihrem PowerVault™ ML6000 ein (German)

Info über Vorsichtshinweise

VORSICHT: VORSICHT weist darauf hin, dass es bei Nichtbefolgung der Anweisungen zu potenziellen Schäden an der Hardware oder zu Datenverlust kommen kann.

Zweck dieses Dokuments

Dell Encryption Key Manager (EKM) ist eine zentrale Schlüsselverwaltungsanwendung, in der jene Schlüssel verwaltet werden, die als Teil des IBM LTO-4- und des laufwerksbasierten IBM LTO-5-Datenverschlüsselungsvorgangs verwendet werden. Die bibliotheksverwaltete Verschlüsselung ist eine optionale, lizenzierte Funktion, die über die PowerVault ML6000-Bibliothek aktiviert werden muss, damit die Verschlüsselung von Daten mithilfe der LTO-4/LTO-5-Bandlaufwerks-Verschlüsselungsfähigkeiten beginnen kann.

Der Dell EKM ist ein IBM-Java-Softwareprogramm, das für Verschlüsselung aktivierte Bandlaufwerke bei der Erstellung, Sicherung, Speicherung und Wartung von Verschlüsselungsschlüsseln hilft, mit denen auf Bandmedien geschriebene Informationen verschlüsselt bzw. von Bandmedien gelesene Informationen entschlüsselt werden. Richtliniensteuerung und Schlüssel durchlaufen die Bibliothek, daher ist die Verschlüsselung für die Anwendungen transparent.

Weitere Information zum Installieren und Konfigurieren des EKM-Servers und den Best Practices von Dell EKM finden Sie im *Benutzerhandbuch zu Dell PowerVault Encryption Key Manager* und dem Datenblatt *Dell Encryption Key Manager and Library Managed Encryption Best Practices and FAQ*.

ANMERKUNG: Um ein ordnungsgemäßes Funktionieren des Dell EKM zu gewährleisten, müssen sowohl die Bibliothek als auch die Bandlaufwerk-Firmware auf die jeweils aktuellen Versionen aktualisiert werden. Die neueste Firmware sowie Installationsanweisungen sind unter http://support.dell.com verfügbar.

Unterstützte Bandlaufwerke und Datenträger

Die bibliotheksverwaltete Verschlüsselung in PowerVault ML6000 unterstützt lediglich die Verschlüsselung von LTO-4- und LTO-5-Datenkassetten, die IBM LTO-4- und LTO-5 Fibre Channel- und SAS-Bandlaufwerke verwenden. Die Verschlüsselung auf anderen Bandlaufwerkstypen oder Herstellermarken wird von der bibliotheksverwalteten ML6000-Verschlüsselung nicht unterstützt, selbst dann nicht, wenn sie einer zur Verschlüsselung ausgewählten Partition zugewiesen sind. Andere Datenträgertypen (z. B. LTO-3) können von Bandlaufwerken, die für die bibliotheksverwaltete Verschlüsselung aktiviert wurden, zwar gelesen, jedoch nicht verschlüsselt werden.

Installieren von Dell EKM auf einem Server

Sie müssen einen oder mehrere Server bereitstellen, auf dem bzw. denen Dell EKM installiert werden soll. Beim Kauf der bibliotheksverwalteten Verschlüsselung erhalten Sie eine CD, die die auf dem Server zu installierende Software sowie Installationsanweisungen und ein Benutzerhandbuch enthält. Sie müssen Ihre EKM-Server einrichten und Ihren Lizenzschlüssel installieren, bevor Sie EKM bei Ihrer Bibliothek einrichten können.

ANMERKUNG: Da die Dell PowerVault ML6000-Bibliothek beim Lesen von oder Schreiben auf einem für Verschlüsselung aktivierten Bandlaufwerk in Echtzeit mit dem EKM-Server kommunizieren muss, wird dringend empfohlen, einen primären und einen sekundären EKM-Server zu verwenden. Auf diese Weise kann der sekundäre Server die Aufgabe übernehmen, wenn der primäre Server nicht zur Verfügung steht, wenn die Bibliothek Verschlüsselungsinformationen benötigt. Die Dell PowerVault ML6000-Bibliothek ermöglicht die Verwendung von bis zu zwei EKM-Servern für Ausfallsicherungs-/Redundanzzwecke.

Einrichten der Verschlüsselung auf der Bibliothek

Schritt 1: Installation eines Lizenzschlüssels

ANMERKUNG: Stellen Sie sicher, dass die Bibliothek und die Bandlaufwerk-Firmware auf die jeweils aktuellen Versionen aktualisiert sind. Aktuelle Anleitungen zu Firmware und Installation stehen unter www.support.dell.com zur Verfügung.

1. Fordern Sie mit Hilfe der erhaltenen Anleitungen in dem *EKM License Key Certificate (EKM-Lizenzschlüsselzertifikat)* einen Lizenzschlüssel für die Verschlüsselung an.
2. Führen Sie einen der folgenden Schritte durch:
   - Wählen Sie auf dem Bedienfeld **Setup > Licenses (Setup > Lizenzen)** aus.
   - Wählen Sie im Webclient **Setup > License (Setup > Lizenz)** aus.
3. Geben Sie den neuen Lizenzschlüssel ein.
4. Klicken Sie auf **Apply (Anwenden)**.

   Es wird ein Statusfenster eingeblendet, das die verstrichene Zeit anzeigt. Nach Beendigung erscheint die grüne Meldung **Success (Erfolg)**, worauf der Status zu "Operation Succeeded" ("Vorgang erfolgreich durchgeführt") geändert wird. Die Verschlüsselung wird jetzt auf dem Bildschirm als Funktion aufgeführt. (Wird die Meldung **Failure (Fehler)** eingeblendet, haben Sie möglicherweise einen falschen Lizenzschlüssel eingegeben.)
5. Klicken Sie auf **Close (Schließen)**.

Schritt 2: Konfigurieren von Verschlüsselungsschlüsseln und Schlüssel-Serveradressen

1. Nehmen Sie die Bandkassetten aus allen verschlüsselungsfähigen Bandlaufwerken in der Bibliothek.
2. Wählen Sie vom Webclient aus **Setup > Encryption > System Configuration (Setup > Verschlüsselung > Systemkonfiguration)** aus.
3. **Automatische EKM-Pfaddiagnose**: Aktivieren oder deaktivieren Sie diese Funktion und stellen Sie das gewünschte Testintervall ein. Sie können auch die Anzahl der nacheinander verpassten Testintervalle angeben, die zur Generierung eines Rücksendegenehmigungstickets erforderlich sind. Weitere Informationen finden Sie unter Automatische EKM-Pfaddiagnose auf Seite 24EKM Path Diagnostics (EKM-Pfaddiagnose).
4. **Secure Sockets Layer (SSL)**: Zum Aktivieren von SSL für die Kommunikation zwischen der Bibliothek und den EKM-Schlüsselservern markieren Sie das Kontrollkästchen **SSL-Verbindung**. Die Standardeinstellung ist Disabled (Deaktiviert). Wenn Sie SSL aktivieren, müssen Sie sicherstellen, dass die Anschlussnummern des primären und sekundären Schlüsselservers (siehe unten) mit den SSL-Anschlussnummern der EKM-Schlüsselserver übereinstimmen. Die Standard-SSL-Anschlussnummer ist 443.

ANMERKUNG: Schlüssel sind immer verschlüsselt, bevor sie vom EKM-Schlüsselserver an ein Bandlaufwerk gesendet werden, unabhängig davon, ob SSL aktiviert ist oder nicht. Aktivierung von SSL bringt zusätzliche Sicherheit.

5. Geben Sie in das Textfeld **Primary Key Server IP Address or Host (IP-Adresse oder Host des primären Schlüsselservers)** Folgendes ein:
   - Die IP-Adresse des primären Schlüsselservers, wenn DNS nicht aktiviert ist, oder
   - Den Hostnamen des primären Schlüsselservers, wenn DNS aktiviert ist
6. Geben Sie die Anschlussnummer des primären Servers in das Textfeld **Primary Key Server Port Number (Anschlussnummer des primären Schlüsselservers)** ein. Die Standardanschlussnummer ist 3801, wenn SSL nicht aktiviert ist. Ist SSL aktiviert, lautet die Standardanschlussnummer 443.

ANMERKUNG: Wenn Sie die festgelegte Anschlussnummer in der Bibliothek ändern, müssen Sie auch die Nummer im Schlüsselserver ändern, damit sie übereinstimmen. Andernfalls funktioniert EKM nicht ordnungsgemäß.

7. Wenn Sie zu Ausfallsicherungszwecken einen sekundären Schlüsselserver verwenden, geben Sie dessen IP-Adresse oder Hostnamen in das Textfeld **Secondary Key Server IP Address or Host (IP-Adresse oder Host des sekundären Schlüsselservers)** ein.

ANMERKUNG: Wenn Sie nicht beabsichtigen, einen sekundären Schlüsselserver zu verwenden, können Sie in das Textfeld **Secondary Key Server IP Address or Host (IP-Adresse oder Host des sekundären Schlüsselservers)** eine aus Nullen bestehende IP-Adresse (0.0.0.0) eingeben oder das Feld leer lassen.

8. Wenn Sie im vorherigen Schritt einen sekundären Schlüsselserver konfiguriert haben, geben Sie dessen Anschlussnummer in das Textfeld **Secondary Key Server Port Number (Anschlussnummer des sekundären Schlüsselservers)** ein. Die Standardanschlussnummer ist 3801, wenn SSL nicht aktiviert ist. Ist SSL aktiviert, lautet die Standardanschlussnummer 443.

ANMERKUNG: Bei Verwendung eines sekundären Schlüsselservers muss die Anschlussnummer des primären und des sekundären Schlüsselservers identisch sein. Andernfalls findet keine Synchronisierung und keine Ausfallsicherung statt.

9 Klicken Sie auf **Apply (Anwenden)**.

Das Statusfenster wird geöffnet. Das Statusfenster enthält Informationen zu Aktion, verstrichener Zeit und Status des Vorgangs. Führen Sie einen der folgenden Schritte durch:

- Wenn im Statusfenster **Success (Erfolg)** angezeigt wird, wurden die Systemeinstellungen des EKM erfolgreich konfiguriert. Klicken Sie auf **Close (Schließen)**, um das Statusfenster zu schließen.
- Wenn im Statusfenster **Failure (Fehler)** angezeigt wird, konnten die Systemeinstellungen des EKM nicht erfolgreich konfiguriert werden. Befolgen Sie die im Statusfenster aufgeführten Anleitungen zum Lösen von Problemen, die während des Vorgangs aufgetreten sind.

ANMERKUNG: Wenn Sie beabsichtigen, unterschiedliche EKM-Schlüsselserver für unterschiedliche Partitionen zu verwenden, müssen Sie auch den Abschnitt für die Außerkraftsetzung im Bildschirm **Setup > Encryption > Partition Encryption (Setup > Verschlüsselung > Partitionsverschlüsselung)** ausfüllen. Weitere Informationen finden Sie unter Schritt 3: Konfiguration der Partitionsverschlüsselung.

Schritt 3: Konfiguration der Partitionsverschlüsselung

Die Verschlüsselung in der Dell PowerVault ML6000-Bandbibliothek wird nur partitionsweise aktiviert. Es können keine individuellen Bandlaufwerke zur Verschlüsselung ausgewählt werden, dazu muss eine vollständige Partition gewählt werden. Wenn Sie eine Partition für die bibliotheksverwaltete Verschlüsselung auswählen, werden alle Bandlaufwerke in der Partition, die die bibliotheksverwaltete Verschlüsselung unterstützen, ebenfalls ausgewählt und alle darauf geschriebenen Daten werden verschlüsselt. Bandlaufwerke, die in dieser Partition nicht von der bibliotheksverwalteten Verschlüsselung unterstützt werden, werden nicht für die Verschlüsselung aktiviert und die darauf geschriebenen Daten werden nicht verschlüsselt.

Daten, die auf für Verschlüsselung unterstützte und verschlüsselungsfähige Datenträger in bibliotheksverwalteten und für Verschlüsselung unterstützten Bandlaufwerken geschrieben werden, werden verschlüsselt, *es sei denn*, die Daten wurden zuvor in unverschlüsseltem Format auf den Datenträger geschrieben. Damit die Daten verschlüsselt werden können, muss der Datenträger leer sein oder der erste Schreibvorgang muss am Beginn des Bandes mit einer bibliotheksverwalteten Verschlüsselung erfolgt sein.

Konfigurieren Sie die Partition(en) wie folgt:

1 Wählen Sie vom Webclient aus **Setup > Encryption > Partition Configuration (Setup > Verschlüsselung > Partitionskonfiguration)**.

Es wird eine Liste aller Partitionen zusammen mit einer Dropdown-Liste angezeigt, die die Verschlüsselungsmethode für jede Partition enthält.

2 Wenn Sie die Verschlüsselungsmethode für eine Partition ändern möchten, vergewissern Sie sich, dass sich in keinem der Bandlaufwerke in dieser Partition eine Kassette befindet. Befindet sich eine Kassette in einem Bandlaufwerk, kann die Verschlüsselungsmethode nicht geändert werden.

3 Wählen Sie für jede Partition eine Verschlüsselungsmethode aus der Dropdown-Liste aus. Bei Bandlaufwerken, die die Verschlüsselung unterstützen, lautet die Standardeinstellung **Application Managed (Anwendungsverwaltet)**. Die Verschlüsselungsmethode wird auf alle verschlüsselungsfähigen Bandlaufwerke und Datenträger in der jeweiligen Partition angewendet.

Verschlüsselungsmethode	Beschreibung
Library Managed (Bibliotheksverwaltet)	**For use with EKM (Zur Verwendung mit EKM).** Aktiviert die Verschlüsselungsunterstützung über einen verbundenen Dell EKM-Schlüsselserver für alle verschlüsselungsfähigen Bandlaufwerke und Datenträge, die der Partition zugewiesen sind.
Application Managed (Anwendungsverwaltet)	**Not for use with EKM (Nicht zur Verwendung mit EKM).** Ermöglicht es einer externen Sicherungsanwendung, allen verschlüsselungsfähigen Bandlaufwerken und Datenträgern in der Partition Verschlüsselungsunterstützung bereitzustellen. Die Bibliothek wird NICHT mit dem Dell EKM-Server auf dieser Partition kommunizieren. Dies ist die Standardeinstellung, wenn sich in der Partition verschlüsselungsfähige Bandlaufwerke befinden. Diese Option sollte ausgewählt bleiben, *es sei denn* Sie möchten, dass Dell EKM die Verschlüsselung verwaltet. **ANMERKUNG:** Wenn Sie möchten, dass eine Anwendung die Verschlüsselung verwaltet, ist es notwendig, dass Sie die Anwendung speziell zu diesem Zweck konfigurieren. Die Bibliothek nimmt am Ausführen dieser Art von Verschlüsselung nicht teil.

None (Ohne)	Deaktiviert die Verschlüsselung der Partition.
Unsupported (Nicht unterstützt)	Bedeutet, dass keine Bandlaufwerke in dieser Partition die Verschlüsselung unterstützen. **Unsupported (Nicht unterstützt)** ist grau unterlegt, falls angezeigt. Die Einstellung kann nicht geändert werden.

4 Wenn unterschiedliche Partitionen unterschiedliche EKM-Schlüsselserver verwenden sollen, füllen Sie den Abschnitt Library Managed Encryption Server Overrides (Bibliotheksverwalteten Verschlüsselungsserver außer Kraft setzen) aus, wie in diesem Abschnitt beschrieben. Die Einstellungen im Abschnitt für das Außerkraftsetzen treten an die Stelle der Standardeinstellungen im Bildschirm **Setup > Encryption > System Configuration (Setup > Verschlüsselung > Systemkonfiguration)**. (Die Einstellungen im Überschreibungsabschnitt ändern jedoch nicht die Einstellungen, die auf dem Bildschirm **Setup > Encryption > System Configuration (Setup > Verschlüsselung > Systemkonfiguration)** aufgeführt werden. Diese Einstellungen sind die Standardkonfigurationseinstellungen für jede Partition, die keine Überschreibungen verwendet.) Überschreibungen sind nur auf Partitionen verfügbar, bei denen **Library Managed (Bibliotheksverwaltet)** als Verschlüsselungsmethode festgelegt ist.

VORSICHT: Füllen Sie den Abschnitt für das Außerkraftsetzen nur dann aus, wenn unterschiedliche Partitionen unterschiedliche EKM-Schlüsselserver verwenden sollen. Verändern Sie ansonsten nichts an diesem Abschnitt und lassen Sie diese Felder mit den Werten des Bildschirms Setup > Encryption > System Configuration (Einrichten > Verschlüsselung > Systemkonfiguration) ausfüllen. Sobald Sie Änderungen am Überschreibungsabschnitt vorgenommen haben, werden diese Felder nicht mehr automatisch mit den Standardwerten des Bildschirms Setup > Encryption > System Configuration (Einrichten > Verschlüsselung > Systemkonfiguration) ausgefüllt. Wenn Sie die Standardeinstellungen wiederherstellen möchten, nachdem Sie die Überschreibungen geändert haben, müssen Sie diese manuell eingeben.

Gehen Sie bei jeder Partition, für die Library Managed (Bibliotheksverwaltet) als Verschlüsselungsmethode festgelegt ist, folgendermaßen vor:

- Geben Sie die IP-Adresse (wenn DNS nicht aktiviert ist) bzw. den Hostnamen (wenn DNS aktiviert ist) des primären EKM-Schlüsselservers in das Textfeld **Primary Host (Primärer Host)** ein.
- Geben Sie die Anschlussnummer des primären EKM-Schlüsselservers in das Feld **Port (Anschluss)** ein. Die Standardanschlussnummer ist 3801, wenn SSL nicht aktiviert ist. Ist SSL aktiviert, lautet die Standardanschlussnummer 443.
- Geben Sie bei Verwendung eines sekundären EKM-Servers dessen Adresse/Hostname und Anschlussnummer in die Textfelder **Secondary Host (Sekundärer Host)** und **Port (Anschluss)** ein.
- Wählen Sie das Kontrollkästchen **SSL**, wenn Sie SSL für die Kommunikation zwischen dieser Partition und den EKM-Servern aktivieren möchten. Die Standardeinstellung ist Disabled (Deaktiviert). Wenn Sie SSL aktivieren, müssen Sie sicherstellen, dass die Anschlussnummer des primären und des sekundären EKM-Servers im Abschnitt für das Außerkraftsetzen mit den SSL-Anschlussnummern der EKM-Server übereinstimmen. Die Standard-SSL-Anschlussnummer ist 443.

ANMERKUNG: Schlüssel werden immer verschlüsselt, bevor sie vom EKM-Server an ein Bandlaufwerk gesendet werden, ob SSL aktiviert ist oder nicht. Aktivierung von SSL bringt zusätzliche Sicherheit.

ANMERKUNG: Einschränkung für EKM-Server, die zur Außerkraftsetzung verwendet werden: Wenn Sie zum Außerkraftsetzen primäre und sekundäre Server verwenden, gilt die folgende Einschränkung. (Wenn Sie keinen Sekundärserver verwenden, bestehen keinerlei Einschränkungen.)

Einschränkung: Ein bestimmter Primärserver und ein Sekundärserver müssen „gepaart" werden und können nicht in unterschiedlichen Kombinationen verwendet werden. Beispiel:
- Server1 kann den primären und Server2 den sekundären Server in einigen oder allen Partitionen darstellen.
- Wenn Server1 dem primären und Server2 dem sekundären Server entspricht, kann Server1 in jeder beliebigen anderen Partition, in der Sie ihn verwenden, immer nur der primäre Server sein und muss mit Server2 als sekundären Server „gepaart" werden. In einer anderen Partition kann Server1 nicht der primäre und Server3 der sekundäre Server sein.
- Server1 kann nicht sowohl der primäre Server in PartitionA als auch der sekundäre Server in PartitionB sein.
- Server2 kann nicht sowohl der sekundäre Server in PartitionA als auch der primäre Server in PartitionB sein.

Wenn Sie Außerkraftsetzungen verwenden, stellen Sie sicher, dass Sie Dell EKM auf allen von Ihnen angegebenen Servern installieren. Führen Sie anschließend die manuelle EKM-Pfaddiagnose auf allen Bandlaufwerken in allen für EKM konfigurierten Partitionen durch, um sicherzustellen, dass jedes Bandlaufwerk mit dem angegebenen EKM-Schlüsselserver kommunizieren und von ihm Schlüssel erhalten

www.dell.com | support.dell.com

kann. Weitere Informationen finden Sie unter Verwendung der EKM-Pfaddiagnose auf Seite 22EKM Path Diagnostics (EKM-Pfaddiagnose).

5 Klicken Sie auf **Apply (Anwenden)**.

Das Statusfenster wird eingeblendet. Das Statusfenster enthält Informationen zu Aktion, verstrichener Zeit und Status des angeforderten Vorgangs. Führen Sie einen der folgenden Schritte durch:

- Wenn im Statusfenster **Success (Erfolg)** angezeigt wird, wurden die Systemeinstellungen des EKM erfolgreich konfiguriert. Klicken Sie auf **Close (Schließen)**, um das Statusfenster zu schließen.
- Wenn im Statusfenster **Failure (Fehler)** angezeigt wird, konnten die Systemeinstellungen des EKM nicht erfolgreich konfiguriert werden. Befolgen Sie die im Statusfenster aufgeführten Anleitungen zum Lösen von Problemen, die während des Vorgangs aufgetreten sind.

6 Speichern Sie die Bibliothekskonfiguration (Anleitungen befinden sich im *Dell PowerVault ML6000-Benutzerhandbuch*).

Schritt 4: Durchführen der EKM-Pfaddiagnose

Führen Sie die EKM-Pfaddiagnose durch, um sicherzustellen, dass die Bandlaufwerke und Schlüsselserver angeschlossen sind und ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter Verwendung der EKM-Pfaddiagnose auf Seite 22.

Sicherung von Keystore-Daten

Da Ihr Keystore sehr kritische Schlüssel enthält, ist es überaus wichtig, Ihre Keystore-Daten auf einem unverschlüsselten Gerät zu sichern, damit Sie sie bei Bedarf wiederherstellen und die Bänder lesen können, die mit dem zum jeweiligen Bandlaufwerk oder der Bibliothek gehörenden Schlüssel verschlüsselt wurden.

Verwendung der EKM-Pfaddiagnose

Die EKM-Pfaddiagnose besteht aus einer Reihe kurzer Tests, mit denen festgestellt wird, ob die Schlüsselserver laufen, verbunden und in der Lage sind, entsprechend der Erfordernis Schlüssel zu liefern.

Führen Sie die manuelle EKM-Pfaddiagnose jedes Mal durch, wenn Sie die Einstellungen des Schlüsselservers oder der Bibliotheksverschlüsselung ändern sowie bei jedem Austausch eines Bandlaufwerks. Es wird empfohlen, alle Laufwerke zu testen, die mit Schlüsselmanagerservern kommunizieren.

Die Diagnose besteht aus den folgenden Tests:

ANMERKUNG: Damit die Tests durchgeführt werden können, muss das getestete Bandlaufwerk leer, bereit und online sein.

- **Ping** – Überprüft die Ethernet-Kommunikationsverbindung zwischen der Bibliothek und den Schlüsselservern. Falls die Partition, auf der sich das ausgewählte Bandlaufwerk befindet, Außerkraftsetzungen von EKM-Servern verwendet, müssen die IP-Adressen der Außerkraftsetzungen getestet werden (s. **Setup > Encryption > Partition Configuration (Einrichten > Verschlüsselung > Partitionskonfiguration)**). Verwendet die Partition keine Außerkraftsetzungen, werden die Standardsystem-IP-Adressen geprüft (s. **Setup > Encryption > System Configuration (Einrichten > Verschlüsselung > Systemkonfiguration)**).
- **Drive (Laufwerk)** – Überprüft den Pfad des Bandlaufwerks in der Bibliothek (Kommunikation von der Bibliothek zum Bandlaufwerksschlitten und vom Bandlaufwerksschlitten zum Bandlaufwerk). Damit dieser Test durchgeführt werden kann, muss das Bandlaufwerk leer, bereit und online sein. Wenn dieser Test fehlschlägt, werden der Path- und der Config-Test nicht durchgeführt.
- **Path (Pfad)** – Überprüft, ob die EKM-Dienste auf den Schlüsselservern ausgeführt werden. Dieser Test kann nicht durchgeführt werden, wenn der Drive-Test fehlschlägt.
- **Config (Konfiguration)** – Überprüft, ob die Schlüsselserver in der Lage sind, Verschlüsselungsschlüssel zu liefern. Dieser Test kann nicht durchgeführt werden, wenn der Drive-Test fehlschlägt.

Wenn einer der Tests fehlschlägt, probieren Sie die folgenden Lösungen, und führen Sie den Test erneut aus, um sicherzustellen, dass dieser abgeschlossen wird:

- **Fehlschlagen des Ping-Tests** – Überprüfen Sie, ob der Schlüsselserver-Host läuft und vom Netzwerk aus, mit dem die Bibliothek verbunden ist, auf ihn zugegriffen werden kann.
- **Fehlschlagen des Drive-Tests** – Suchen Sie nach Bandlaufwerk-Rücksendegenehmigungstickets und befolgen Sie die dortigen Auflösungsanweisungen.

- **Fehlschlagen des Path-Tests** – Überprüfen Sie, ob der Schlüsselserver läuft und die Anschluss-/SSL-Einstellungen mit den Konfigurationseinstellungen der Bibliothek übereinstimmen.
- **Fehlschlagen des Config-Tests** – Überprüfen Sie, ob der EKM-Server so eingerichtet ist, dass er das getestete Bandlaufwerk akzeptiert.

Die Diagnose kann auf zwei Arten durchgeführt werden:

- Manuelle EKM-Pfaddiagnose
- Automatische EKM-Pfaddiagnose

Die manuelle Diagnose unterscheidet sich folgendermaßen von der automatischen Diagnose:

- Bei der manuellen Diagnose werden die betroffenen Partitionen offline gebracht. Bei der automatischen Diagnose bleiben die Partitionen online. Während des Tests können sich Bewegungen auf die Bandlaufwerke verzögern.
- Bei der manuellen EKM-Pfaddiagnose muss ein Bandlaufwerk für den Test ausgewählt werden. Da beim Test lediglich das ausgewählte Laufwerk überprüft wird, müssen Sie den Test mehrmals (d. h. einmal pro Laufwerk) durchführen, wenn alle Pfade für alle Bandlaufwerke getestet werden sollen. Zum Testen aller Server müssen Sie die Diagnose für jede für die bibliotheksverwaltete Verschlüsselung aktivierte Partition einmal durchführen (jedes Serverpaar ist mit einer einzigen Partition und einem Bandlaufwerk verbunden). Wenn das Bandlaufwerk nicht verfügbar ist (es muss leer, bereit und online sein), wird der Drive-, Path- und Config-Test nicht durchgeführt.
- Bei der automatischen EKM-Pfaddiagnose wird nacheinander jeder verbundene EKM-Server getestet und die Bibliothek wählt das Bandlaufwerk aus, das für jeden Test verwendet werden soll. Wenn das ausgewählte Bandlaufwerk nicht verfügbar ist (es muss leer, bereit und online sein), probiert die Bibliothek ein anderes mit dem Schlüsselserver verbundenes Bandlaufwerk aus, bis sie eins findet, das verfügbar ist. Wenn keine mit einem bestimmten Schlüsselserver verbundenen Bandlaufwerke verfügbar sind, wird dieser Server übergangen und die Tests werden nicht durchgeführt. Wenn ein Server während „X“ aufeinanderfolgender Testintervalle („X“ kann auf dem Webclient konfiguriert werden) übergangen wird, generiert die Bibliothek ein Rücksendegenehmigungsticket. Wenn ein Bandlaufwerk über lange Zeit beladen ist, wird es möglicherweise nie getestet. Wenn Sie ein bestimmtes Bandlaufwerk testen möchten, sollten Sie die manuelle EKM-Pfaddiagnose durchführen. Die manuelle EKM-Pfaddiagnose sollte insbesondere nach dem Austausch eines Bandlaufwerks durchgeführt werden.

Manuelle EKM-Pfaddiagnose

1. Sie können auf zwei Arten auf den Bildschirm „EKM Path Diagnostics“ (EKM-Pfaddiagnose) zugreifen:
   - Öffnen Sie die Bibliotheksdiagnose (wählen Sie **Tools > Diagnostics (Extras > Diagnose)**) und wählen Sie anschließend **EKM > EKM Path Diagnostics (EKM > EKM-Pfaddiagnose)**. Beim Öffnen der Diagnose werden alle Benutzer mit denselben oder niedrigeren Zugriffsberechtigungen abgemeldet und die Partitionen werden offline gebracht. Nach dem Schließen der Diagnose werden die Partitionen automatisch wieder online gebracht.
   - Wählen Sie **Setup > Encryption > System Configuration (Setup > Verschlüsselung > Systemkonfiguration)** oder **Setup > Encryption > Partition Configuration (Setup > Verschlüsselung > Partitionskonfiguration)** und klicken Sie auf die Verknüpfung mit dem Text „Click here to run EKM Path Diagnostics“ (Klicken Sie hier, um die EKM-Pfaddiagnose durchzuführen). Bei Durchführung dieser Aktion wird die Partition, auf der sich das ausgewählte Bandlaufwerk befindet, offline gebracht. Wenn der Test abgeschlossen ist, geht die Partition automatisch wieder online.

   Es wird eine Liste mit allen Bandlaufwerken angezeigt, die für bibliotheksverwaltete Verschlüsselung aktiviert sind, zusammen mit dem Bandlaufwerkstatus und der Partition, auf der sich jedes Bandlaufwerk befindet.
2. Wählen Sie das Bandlaufwerk aus, bei dem eine Diagnose ausgeführt werden soll, und klicken Sie auf **Apply (Anwenden)**. Damit der Test durchgeführt werden kann, muss das Bandlaufwerk leer, bereit und online sein.

   Es wird ein Dialogfeld aufgerufen, welches angibt, dass die ausgewählte Partition offline genommen wird.
3. Klicken Sie auf **OK**, um die Diagnose zu starten.

   Das Statusfenster wird eingeblendet. Das Statusfenster enthält Informationen zu Aktion, verstrichener Zeit und Status des angeforderten Vorgangs.

   Die Bibliothek führt die Diagnose aus und meldet alle Bestanden/Fehler-Ergebnisse zu jedem der Tests im Fortschrittsfenster an.

www.dell.com | support.dell.com

ANMERKUNG: Diagnosetests dauern möglicherweise mehrere Minuten, bis sie abgeschlossen sind.

4 Führen Sie einen der folgenden Schritte durch:

- Wenn im Fortschrittsfenster **Completed (Abgeschlossen)** angezeigt wird, wurde die Diagnose durchgeführt (das bedeutet nicht, dass die Diagnose erfolgreich war, sondern lediglich, dass sie überhaupt durchgeführt wurde). Klicken Sie auf **Close (Schließen)**, um das Statusfenster zu schließen.
- Wenn **Failure (Fehler)** im Fortschrittsfenster angezeigt wird, konnte die Diagnose nicht ausgeführt werden. Befolgen Sie die im Statusfenster aufgeführten Anleitungen zum Lösen von Problemen, die während des Vorgangs aufgetreten sind.

Automatische EKM-Pfaddiagnose

Sie können die Bibliothek für die Durchführung der automatischen EKM-Pfaddiagnose zu festgelegten Intervallen aktivieren. In jedem Intervall testet die Bibliothek jeden konfigurierten Schlüsselserver. Im Fall von Problemen, generiert die Bibliothek ein Rücksendegenehmigungsticket. Diese Funktion ist standardmäßig deaktiviert. Das Standard-Testintervall beträgt vier Stunden. Es wird empfohlen, die automatische EKM-Pfaddiagnose deaktiviert zu belassen, es sei denn, es treten häufig Verschlüsselungsfehler aufgrund von Netzwerkunterbrechungen auf.

VORSICHT: Bei der Durchführung der automatischen EKM-Pfaddiagnose können vermehrt Rücksendegenehmigungstickets generiert werden, wenn Tests übersprungen werden, weil Bandlaufwerke während mehrerer aufeinanderfolgender konfigurierbarer Testintervalle nicht verfügbar sind. Um die Generierung von Rücksendegenehmigungstickets zu reduzieren, können Sie die Anzahl der aufeinanderfolgenden Testintervalle, die für die Generierung eines Rücksendegenehmigungstickets erforderlich sind, erhöhen oder die Bibliothek so einstellen, dass keine Rücksendegenehmigungstickets für ausgelassene Testintervalle generiert werden.

Eine Liste der durchgeführten Tests finden Sie unter Verwendung der EKM-Pfaddiagnose auf Seite 22.

So aktivieren Sie die automatische EKM-Pfaddiagnose:

1 Wählen Sie vom Webclient aus **Setup > Encryption > System Configuration (Setup > Verschlüsselung > Systemkonfiguration)** aus.

2 Markieren Sie das Kontrollkästchen **Automatic EKM Path Diagnostics (Automatische EKM-Pfaddiagnose)**.

3 Wählen Sie aus der Dropdown-Liste ein Intervall aus.

4 Geben Sie die Anzahl der aufeinanderfolgenden ausgelassenen Testintervalle an, die für die Generierung eines Rücksendegenehmigungstickets erforderlich sind, in dem Sie darüber informiert werden, dass der Test nicht innerhalb der festgelegten Intervalle durchgeführt werden konnte.

Anzeigen der Verschlüsselungseinstellungen des Bandlaufwerks

Die Verschlüsselungseinstellungen können folgendermaßen angezeigt werden:

- **System Information Report (Systeminformationsbericht -** Zur Anzeige von Verschlüsselungsinformationen zu allen Schlüsselservern, Partitionen und Bandlaufwerken wählen Sie im Webclient **Reports > System Information (Berichte > Systeminformationen)**. Weitere Informationen finden Sie im *Dell PowerVault ML6000-Benutzerhandbuch*.
- **Library Configuration Report (Bibliothekskonfigurationsbericht) -** Zur Anzeige des Verschlüsselungsstatus eines ausgewählten Bandlaufwerks oder einer Bandkassette wählen Sie im Webclient **Reports > Library Configuration (Berichte > Bibliothekskonfiguration)** und klicken auf ein Bandlaufwerk oder einen Schacht. Der Verschlüsselungsstatus wird in einem Popup-Statusfenster angezeigt. Weitere Informationen finden Sie im *Dell PowerVault ML6000-Benutzerhandbuch*.
- **Partition Encryption (Partitionsverschlüsselung) -** Wählen Sie im Webclient **Setup > Encryption > Partition Configuration (Setup > Verschlüsselung > Partitionskonfiguration)**, um die Verschlüsselungseinstellungen von Partitionen anzuzeigen und zu ändern. Weitere Einzelheiten finden Sie in Schritt 3: Konfiguration der Partitionsverschlüsselung auf Seite 20.

LEA ESTO PRIMERO: Cómo instalar Dell Encryption Key Manager en la biblioteca PowerVault™ ML6000 (Spanish)

Acerca de las precauciones

PRECAUCIÓN: Una PRECAUCIÓN indica daños potenciales al hardware o pérdida de datos si no se siguen las instrucciones.

Objetivo de este documento

Dell Encryption Key Manager (EKM) es una aplicación centralizada que administra las claves de cifrado que se usan como parte del proceso de cifrado de los datos que se guardan en las unidades IBM LTO-4 e IBM LTO-5. El cifrado administrado por biblioteca es una función opcional con licencia que se debe activar desde la biblioteca PowerVault ML6000 a fin de comenzar a cifrar datos mediante la capacidad de cifrado de las unidades de cinta LTO-4/LTO-5.

Dell EKM es un programa de software Java de IBM que ayuda a las unidades de cinta habilitadas para cifrado a generar, proteger, almacenar y mantener las claves de cifrado utilizadas para cifrar la información que se escribe en la cinta y a descifrar la información que se lee de ella. Las claves y el control de políticas pasan a través de la biblioteca; por lo tanto, el cifrado no afecta a las aplicaciones.

Para obtener más información acerca de cómo instalar y configurar el servidor EKM y conocer las prácticas recomendadas de Dell EKM, consulte la *Guía del usuario de Dell PowerVault Encryption Key* y la hoja de datos *Preguntas frecuentes y prácticas recomendadas de Dell Encryption Key Manager y del cifrado administrado por la biblioteca*.

NOTA: Para que Dell EKM funcione adecuadamente, usted deberá actualizar el firmware de la biblioteca y de la unidad para que tengan las versiones que se han publicado más recientemente. El firmware más reciente y las instrucciones de instalación están disponibles en http://support.dell.com.

Unidades de cinta y medios compatibles

El cifrado administrado por biblioteca en PowerVault ML6000 admite el cifrado solamente en los cartuchos de datos LTO-4 y LTO-5 que usan unidades de cinta Fibre Channel y SAS IBM LTO-4 y LTO-5. El cifrado administrado por biblioteca en PowerVault ML6000 no admite el cifrado de otros tipos de unidades de cinta o marcas de fabricantes, aun cuando las unidades estén asignadas a una partición seleccionada para cifrado. Otros tipos de medios (por ejemplo, LTO-3) se pueden leer pero no cifrar con las unidades de cinta habilitadas para cifrado administrado por biblioteca.

Instalación de Dell EKM en un servidor

Debe proporcionar un servidor o servidores en los que se instalará Dell EKM. Cuando adquiere el cifrado administrado por biblioteca, también recibe un CD que contiene el software que se debe instalar en el servidor, junto con las instrucciones de instalación y una guía del usuario. Debe configurar los servidores EKM e instalar su clave de licencia para poder instalar EKM en su biblioteca.

NOTA: Como la biblioteca Dell PowerVault ML6000 necesita comunicarse con el servidor EKM en tiempo real al leer una unidad de cinta habilitada para cifrado o escribir en ella, se recomienda enfáticamente usar un servidor EKM principal y otro secundario. De esta manera, si el servidor principal no está disponible cuando la biblioteca necesita la información de cifrado, el servidor secundario podrá atender la solicitud. La biblioteca Dell PowerVault ML6000 permite usar hasta dos servidores EKM con fines de conmutación por error/redundancia.

Configuración del cifrado en la biblioteca

Paso 1: Instalación de una clave de licencia

NOTA: Asegúrese de que el firmware de la biblioteca y de la unidad de cinta estén actualizados con las versiones más recientes. El firmware más reciente y las instrucciones de instalación se encuentran en www.support.dell.com.

1. Obtenga una clave de licencia para cifrado siguiendo las instrucciones que aparecen en el *Certificado de clave de licencia* que recibió.
2. Realice una de las siguientes acciones:
   - En el panel del operador, seleccione **Setup (Configuración) > Licenses (Licencias)**.
   - En el cliente web, seleccione **Setup (Configuración) > License (Licencia)**.
3. Introduzca la nueva clave de licencia.
4. Haga clic en **Apply (Aplicar)**.

   Aparecerá una ventana de progreso que muestra el tiempo que ha transcurrido. Cuando termine, aparecerá un mensaje en color verde de **Success (Éxito)** y el estado cambiará a "Operation Succeeded" (Operación satisfactoria). El cifrado aparece ahora como una función en la pantalla. (Si aparece el mensaje **Failure (Error)**, es posible que haya introducido una clave de licencia errónea).
5. Haga clic en **Close (Cerrar)**.

Paso 2: Configuración de los valores de cifrado y las direcciones de servidor de claves

1. Descargue los cartuchos de todas las unidades de cinta con capacidad para cifrado que se encuentran en la biblioteca.
2. En el cliente web, seleccione **Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)**.
3. **Automatic EKM Path Diagnostics (Diagnósticos automáticos de ruta de acceso EKM)**: active o desactive esta función y configure el intervalo de pruebas deseado. También se puede especificar el número de intervalos de pruebas consecutivas omitidos para generar un vale de RAS. Para obtener más información, consulte Diagnósticos automáticos de ruta de acceso EKM en la página 32.
4. **Secure Sockets Layer (SSL) (Capa de sockets seguros [SSL]):** si desea activar SSL para la comunicación entre la biblioteca y los servidores EKM, active la casilla **SSL Connection (Conexión SSL)**. El valor predeterminado es Disabled (Desactivado). Si activa SSL, debe asegurarse de que los **números de puerto del servidor de claves principal** y **secundario** (consulte abajo) coincidan con los números de puerto SSL en los servidores de claves EKM. El número de puerto SSL predeterminado es 443.

NOTA: Las claves siempre se cifran antes de enviarlas desde el servidor de claves EKM a la unidad de cinta, ya sea que SSL esté activada o no. La activación de SSL proporciona seguridad adicional.

5. En el cuadro de texto **Primary Key Server IP Address or Host (Dirección IP o host del servidor de claves principal)**, introduzca una de las siguientes opciones:
   - La dirección IP del servidor de claves principal (si DNS no está activado)
   - El nombre del host del servidor de claves principal (si DNS está activado)
6. Introduzca el número de puerto del servidor de claves principal en el cuadro de texto **Primary Key Server Port Number (Número de puerto del servidor de claves principal)**. El número de puerto predeterminado es 3801, a menos que SSL esté activada. Si SSL está activada, el número de puerto predeterminado es 443.

NOTA: Si cambia la configuración del número de puerto en la biblioteca, también deberá cambiar el número de puerto en el servidor de claves para que coincida; de lo contrario, EKM no funcionará correctamente.

7. Si está usando un servidor de claves secundario para fines de conmutación por error, introduzca la dirección IP o el nombre del host de dicho servidor en el cuadro de texto **Secondary Key Server IP Address or Host (Dirección IP o host del servidor de claves secundario)**.

NOTA: Si no tiene planes de usar un servidor de claves secundario, en el cuadro de texto **Secondary Key Server IP Address or Host (Dirección IP o host del servidor de claves secundario)** puede introducir una dirección IP en ceros, 0.0.0.0, o bien puede dejarlo en blanco.

8 Si configuró un servidor de claves secundario (paso anterior), introduzca el número de puerto para dicho servidor en el cuadro de texto **Secondary Key Server Port Number (Número de puerto del servidor de claves secundario)**. El número de puerto predeterminado es 3801, a menos que SSL esté activada. Si SSL está activada, el número de puerto predeterminado es 443.

NOTA: Si está usando un servidor de claves secundario, los números de puerto para los servidores de claves tanto principal como secundario se deben configurar con el mismo valor. De lo contrario, no tendrán lugar la sincronización ni la conmutación por error.

9 Haga clic en **Apply (Aplicar)**.

Aparecerá la ventana de progreso. La ventana de progreso contiene información sobre la acción, el tiempo transcurrido y el estado de la operación. Realice una de las siguientes acciones:

- Si aparece **Success (Éxito)** en la ventana de progreso, la configuración del sistema EKM fue establecida correctamente. Haga clic en **Close (Cerrar)** para cerrar la ventana de progreso.
- Si aparece **Failure (Error)** en la ventana de progreso, la configuración del sistema EKM no fue establecida correctamente. Siga las instrucciones que aparecen en la ventana de progreso para resolver los problemas que hayan surgido durante la operación.

NOTA: Si planea utilizar diferentes servidores de claves EKM para distintas particiones, también debe completar la sección de anulaciones en la pantalla **Setup (Configuración) > Encryption (Cifrado) > Partition Encryption (Cifrado de particiones)**. Consulte Paso 3: Configuración del cifrado de partición.

Paso 3: Configuración del cifrado de partición

El cifrado en la biblioteca de cintas Dell PowerVault ML6000 sólo está habilitado por partición. No se pueden seleccionar unidades de cinta individuales para cifrado; se debe seleccionar una partición completa para cifrarla. Si activa una partición para cifrado administrado por biblioteca, todas las unidades de cinta que admiten cifrado administrado por biblioteca en la partición quedan habilitadas para el cifrado, y se cifrarán todos los datos escritos en los medios que permiten cifrado en la partición. Cualquier unidad de cinta que no admita cifrado administrado por biblioteca en esa partición no permite el cifrado, y los datos escritos en medios no admitidos no quedan cifrados.

Los datos escritos en medios que admiten el cifrado y que son capaces de ser cifrados en las unidades de cinta que admiten cifrado administrado por biblioteca quedarán cifrados *a menos* que los datos hayan sido previamente escritos en el medio en un formato no cifrado. Para que los datos queden cifrados, el medio debe estar en blanco o haber sido escrito utilizando cifrado administrado por biblioteca durante la primera operación de escritura al comienzo de la cinta (BOT).

Configure las particiones de la siguiente manera:

1 En el cliente web, seleccione **Setup (Configuración) > Encryption (Cifrado) > Partition Configuration (Configuración de partición)**.

Se visualizará una lista de todas las particiones junto con una lista desplegable que muestra el método de cifrado para cada partición.

2 Si desea cambiar el método de cifrado de una partición, asegúrese de que no haya cartuchos cargados en las unidades de cinta de esa partición. Si las unidades de cinta tienen cartuchos cargados, no podrá modificar el método de cifrado.

www.dell.com | support.dell.com

3 Seleccione un método de cifrado en la lista desplegable para cada partición. (En el caso de las unidades de cinta que admiten cifrado, el valor predeterminado es **Application Managed** [**Administrado por aplicación**]). El método de cifrado se aplica a la totalidad de unidades de cinta y medios que admitan cifrado en dicha partición.

Método de cifrado	Descripción
Library Managed (Administrado por biblioteca)	**Para utilizarse con EKM.** Activa la compatibilidad de cifrado por medio de un servidor de claves Dell EKM conectado para todas las unidades de cinta y los medios que se pueden cifrar y que están asignados a la partición.
Application Managed (Administrado por aplicación)	**No debe utilizarse con EKM.** Esta opción permite que una aplicación de copia de seguridad externa proporcione compatibilidad de cifrado a todas las unidades de cinta y los medios que se pueden cifrar en la partición. La biblioteca NO se comunicará con el servidor Dell EKM en esta partición. Es el valor predeterminado cuando usted tiene unidades de cinta que se pueden cifrar en la partición. Esta opción debe permanecer seleccionada *a menos* que desee que Dell EKM administre el cifrado. **NOTA:** Si desea que una aplicación administre el cifrado, deberá configurar la aplicación específicamente para que lo haga. La biblioteca no participará en la realización de este tipo de cifrado.
None (Ninguno)	Desactiva el cifrado en la partición.
Unsupported (No compatible)	Significa que no hay unidades de cinta en la partición que sean compatibles con el cifrado. Si se muestra **Unsupported (No compatible)**, aparecerá inhabilitado y usted no podrá cambiar el valor.

4 Si desea que diferentes particiones utilicen servidores de claves EKM distintos, complete la sección Library Managed Encryption Server Overrides (Anulaciones del servidor de cifrado administrado por biblioteca) conforme se describe en este paso. Los valores de la sección de anulaciones reemplazan los valores predeterminados que se indican en la pantalla **Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)**. (Sin embargo, los valores de las anulaciones no cambian los valores que se indican en la pantalla **Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)**. Esos valores son los valores de configuración predeterminados para cualquier partición que no utilice anulaciones). Las anulaciones sólo están disponibles en las particiones que tienen **Library Managed (Administrada por la biblioteca)** como método de cifrado.

PRECAUCIÓN: Sólo complete la sección de anulaciones si desea que diferentes particiones utilicen servidores de claves EKM distintos. De lo contrario, no complete esta sección y permita que estos campos se llenen con los valores de la pantalla Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema). Una vez que haga estos cambios en la sección anulaciones, los valores predeterminados de la pantalla Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)ya no llenarán estos campos automáticamente. Si desea regresar a los valores predeterminados después de cambiar las anulaciones, deberá introducirlos manualmente.

Para cada partición que tenga Library Managed (Administrado por biblioteca) como método de cifrado, haga lo siguiente:

- Escriba la dirección IP (si DNS no está activado) o el nombre del host (si DNS está activado) del servidor de claves EKM principal en el cuadro de texto **Primary Host (Host principal)**.
- Escriba el número de puerto para el servidor de claves EKM principal en el cuadro de texto **Port (Puerto)**. El número de puerto predeterminado es 3801, a menos que SSL esté activada. Si SSL está activada, el número de puerto predeterminado es 443.

- Si está utilizando un servidor EKM secundario, escriba la dirección/nombre del host y el número de puerto del servidor de claves EKM secundario en los cuadros de texto **Secondary Host (Host secundario)** y **Port (Puerto)**.
- Seleccione la casilla de marcación **SSL** si desea activar la Capa de sockets seguros (SSL) para la comunicación entre esa partición y los servidores EKM. El valor predeterminado es Disabled (Desactivado). Si activa SSL, debe asegurarse de que los números de puerto EKM principal y secundario en la sección de anulaciones coincidan con los números de puerto SSL en los servidores EKM. El número de puerto SSL predeterminado es 443.

NOTA: Las claves se cifran siempre antes de enviarlas desde el servidor EKM a la unidad de cinta, ya sea que SSL esté activada o no. La activación de SSL proporciona seguridad adicional.

NOTA: Restricción en los servidores EKM utilizados para anulaciones: si está utilizando servidores principales y secundarios para las anulaciones, se aplica la siguiente restricción. (Si no está utilizando un servidor secundario, no hay restricciones).

Restricción: se deberá "aparear" un determinado servidor principal con uno secundario y no se pueden usar en distintas combinaciones. Por ejemplo:
• Se puede tener Servidor1 como principal y Servidor2 como secundario para cualquiera o todas las particiones.
• Si Servidor1 es el principal y Servidor2 es el secundario en una partición, entonces en cualquier otra partición que use Servidor1, Servidor1 sólo podrá ser principal y deberá ser "apareado" con Servidor2 como secundario. No se puede tener Servidor1 como principal y Servidor3 como secundario en otra partición.
• No se puede tener Servidor1 como principal en ParticiónA y, a su vez, como secundario en ParticiónB.
• No se puede tener Servidor2 como secundario en ParticiónA y, a su vez, como principal en ParticiónB.

Si utiliza anulaciones, asegúrese de instalar Dell EKM en todos los servidores que especifique. Luego ejecute Manual EKM Path Diagnostics (Diagnósticos manuales de ruta de acceso EKM) en cada unidad de cinta de todas las particiones configuradas para EKM a fin de asegurarse de que cada unidad de cinta se pueda comunicar con el servidor de claves EKM especificado y recibir las claves que éste proporciona. Para obtener más información, consulte Utilización de los diagnósticos de ruta de acceso EKM en la página 30.

5 Haga clic en **Apply (Aplicar)**.

Aparecerá la ventana de progreso. La ventana de progreso contiene información sobre la acción, el tiempo transcurrido y el estado de la operación solicitada. Realice una de las siguientes acciones:

- Si aparece **Success (Éxito)** en la ventana de progreso, la configuración del sistema EKM fue establecida correctamente. Haga clic en **Close (Cerrar)** para cerrar la ventana de progreso.
- Si aparece **Failure (Error)** en la ventana de progreso, la configuración del sistema EKM no fue establecida correctamente. Siga las instrucciones que aparecen en la ventana de progreso para resolver los problemas que hayan surgido durante la operación.

6 Guarde la configuración de la biblioteca (para ver instrucciones, consulte la *Guía del usuario de Dell PowerVault ML6000*).

Paso 4: Ejecución de diagnósticos de ruta de acceso EKM

Ejecute los diagnósticos de ruta de acceso EKM para asegurarse de que las unidades de cinta y los servidores de claves estén conectados y funcionen correctamente. Consulte Utilización de los diagnósticos de ruta de acceso EKM en la página 30.

Copiado de seguridad de los datos del almacén de claves

Debido a la gran importancia de las claves del almacén de claves, es crucial que usted haga una copia de seguridad de los datos del almacén de claves en un dispositivo no cifrado para que pueda recuperarlos cuando sea necesario y para poder leer las cintas que fueron cifradas con las claves de cifrado asociadas a esa biblioteca o unidad de cinta.

www.dell.com | support.dell.com

Utilización de los diagnósticos de ruta de acceso EKM

Los diagnósticos de ruta de acceso EKM constan de una serie de pruebas cortas para validar si los servidores de claves se están ejecutando, están conectados y pueden proporcionar claves según se requiera.

Ejecute los diagnósticos manuales de ruta de acceso EKM cada vez que cambie la configuración del servidor de claves o la configuración de cifrado de la biblioteca, así como cuando reemplace una unidad de cinta. Se recomienda probar cada unidad que se comunique con los servidores del administrador de claves.

Los diagnósticos consisten en las siguientes pruebas:

NOTA: La unidad de cinta usada para la prueba deberá estar descargada, lista y en línea para poder ejecutar cualquiera de las pruebas.

- **Ping**: verifica el enlace de la comunicación Ethernet entre la biblioteca y los servidores de claves. Si la partición en la que reside la unidad de cinta seleccionada utiliza anulaciones del servidor EKM, entonces se prueban las direcciones IP de anulación (consulte **Setup (Configuración) > Encryption (Cifrado) > Partition Configuration (Configuración de particiones)**. Si la partición no utiliza anulaciones, se prueban las direcciones IP predeterminadas del sistema (consulte **Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)**.
- **Drive**: verifica la ruta de acceso de la unidad de cinta en la biblioteca (comunicación desde la biblioteca a la corredera de la unidad de cinta y desde la corredera de la unidad de cinta a la unidad de cinta). La unidad de cinta deberá estar descargada, lista y en línea para poder ejecutar esta prueba. Si esta prueba falla, no se realizan las pruebas de ruta de acceso ni de configuración.
- **Path**: verifica que los servicios de EKM se estén ejecutando en los servidores de claves. Esta prueba no se puede ejecutar si falla la prueba de unidad.
- **Config**: verifica que los servidores de claves puedan proporcionar claves de cifrado. Esta prueba no se puede ejecutar si falla la prueba de unidad.

Si alguna de las pruebas falla, intente las siguientes sugerencias para resolver el problema y vuelva a ejecutar la prueba para asegurarse de que se completa correctamente:

- **Ping Test Failure (Falla de la prueba de ping):** verifique que el host del servidor de claves se esté ejecutando y que sea accesible desde la red a la que está conectada la biblioteca.
- **Drive Test Failure (Falla de la prueba de unidad):** verifique si hay algún vale de RAS para la unidad de cinta y siga las instrucciones de resolución del vale.
- **Path Test Failure (Falla de la prueba de ruta de acceso):** verifique que el servidor de claves efectivamente se esté ejecutando y que los valores del puerto/SSL coincidan con los valores de configuración de la biblioteca.
- **Config Test Failure (Falla de la prueba de configuración):** verifique que el servidor EKM esté configurado para aceptar la unidad de cinta que se está probando.

Este diagnóstico se puede ejecutar de dos formas:

- Diagnósticos manuales de ruta de acceso EKM
- Diagnósticos automáticos de ruta de acceso EKM

Los diagnósticos manuales difieren de los automáticos por lo siguiente:

- Los diagnósticos manuales cambian el estado de las particiones afectadas a "fuera de línea". Los diagnósticos automáticos no cambian el estado de las particiones afectadas a "fuera de línea". Pueden demorar los movimientos de las unidades de cinta mientras se las prueba.
- Para los diagnósticos manuales de ruta de acceso EKM se deberá seleccionar una unidad de cinta que se usará para la prueba. Como la prueba únicamente valida la unidad seleccionada, si se desea probar la ruta de acceso para cada unidad de cinta, se deberá ejecutar esta prueba muchas veces (una vez por cada unidad). Para probar todos los servidores, se deberán ejecutar los diagnósticos una vez para cada partición que permita cifrado administrado por biblioteca (cada par de servidores está conectado a una única partición y unidad de cinta). Si la unidad de cinta no está disponible (debe estar descargada, lista y en línea), no se realizan las pruebas de unidad, ruta de acceso ni configuración.

- Los diagnósticos automáticos de ruta de acceso EKM prueban cada servidor EKM conectado, de a uno por vez, y la biblioteca selecciona la unidad de cinta que se usará para cada prueba. Si la unidad de cinta seleccionada no está disponible (deberá estar descargada, lista y en línea), la biblioteca intenta con otra unidad de cinta que esté conectada al servidor de claves hasta que encuentre una disponible. Si no se dispone de unidades de cinta conectadas a un servidor de claves en particular, ese servidor es omitido y las pruebas no se realizan. Si se omite un servidor durante un número "X" de intervalos de pruebas consecutivas (donde el valor "X" se puede configurar en el cliente web), la biblioteca genera un vale de RAS. Si una unidad de cinta permanece cargada durante mucho tiempo, es posible que nunca se someta a una prueba. Si desea probar una unidad de cinta específica, deberá usar los diagnósticos manuales de ruta de acceso EKM. En particular, si reemplaza una unidad de cinta, ejecute los diagnósticos manuales de ruta de acceso EKM.

Diagnósticos manuales de ruta de acceso EKM

1. Ingrese a la pantalla EKM Path Diagnostics (Diagnósticos de ruta de acceso EKM) de una de las dos formas siguientes:
   - Ingrese a los diagnósticos de biblioteca (seleccione **Tools [Herramientas] > Diagnostics [Diagnósticos]**) y luego seleccione **EKM > EKM Path Diagnostics (Diagnósticos de ruta de acceso EKM)**. Tenga en cuenta que el ingreso a los diagnósticos cerrará la sesión del resto de los usuarios de igual o menor privilegio y cambiará el estado de las particiones a "fuera de línea". Al salir de los diagnósticos, las particiones automáticamente vuelven a estar en línea.
   - Seleccione **Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)** o **Setup (Configuración) > Encryption (Cifrado) > Partition Configuration (Configuración de partición)** y haga clic en el enlace "Click here to run EKM Path Diagnostics" (Haga clic aquí para ejecutar diagnósticos de ruta de acceso EKM). Tenga en cuenta que al realizar esta acción, la partición en la que reside la unidad de cinta seleccionada cambia su estado a "fuera de línea". Cuando la prueba se completa, la partición regresa a su estado de en línea automáticamente.

   Aparece una lista de todas las unidades de cinta activadas para el cifrado administrado por biblioteca, junto con el estado de la unidad de cinta y la partición en la que reside cada unidad de cinta.
2. Seleccione la unidad de cinta en la que desea realizar los diagnósticos y haga clic en **Apply (Aplicar)**. La unidad de cinta debe estar descargada, lista y en línea para que esta prueba se ejecute.

   Aparece un cuadro de diálogo que indica que la partición seleccionada cambiará su estado a fuera de línea.
3. Haga clic en **OK (Aceptar)** para iniciar los diagnósticos.

   Aparecerá la ventana de progreso. La ventana de progreso contiene información sobre la acción, el tiempo transcurrido y el estado de la operación solicitada.

   La biblioteca realiza los diagnósticos e informa los resultados del éxito o falla para cada prueba en la ventana Progress (Progreso).

NOTA: Las pruebas de diagnóstico pueden tardar varios minutos en completarse.

4. Realice una de las siguientes acciones:
   - Si aparece **Completed (Completado)** en la ventana Progress (Progreso), los diagnósticos se llevaron a cabo (esto no significa que los diagnósticos hayan pasado, sólo que se realizaron). Haga clic en **Close (Cerrar)** para cerrar la ventana de progreso.
   - Si aparece **Failure (Error)** en la ventana Progress (Progreso), no fue posible realizar los diagnósticos. Siga las instrucciones que aparecen en la ventana de progreso para resolver los problemas que hayan surgido durante la operación.

www.dell.com | support.dell.com

Diagnósticos automáticos de ruta de acceso EKM

Es posible habilitar la biblioteca para que realice automáticamente los diagnósticos de ruta de acceso EKM a intervalos seleccionados. Durante cada intervalo, la biblioteca prueba todos los servidores de claves configurados. Si hay problemas, la biblioteca genera un vale de RAS. De manera predeterminada, esta función está desactivada. El intervalo de prueba predeterminado es de cuatro horas. Se recomienda dejar desactivados los diagnósticos automáticos de ruta de acceso EKM, a menos que las interrupciones de la red sean una causa común de errores de cifrado en el sitio.

PRECAUCIÓN: La ejecución de diagnósticos automáticos de ruta de acceso EKM puede aumentar los vales de RAS en caso de que las pruebas se omitan porque las unidades de cinta no están disponibles para un número configurable de intervalos de pruebas consecutivas. Para reducir el número de vales de RAS, es posible especificar un valor mayor para el número de intervalos de pruebas consecutivas necesarios para generar un vale de RAS, o también se puede configurar la biblioteca para que nunca genere un vale de RAS para los intervalos de pruebas omitidos.

Si desea ver una lista de las pruebas ejecutadas, consulte Utilización de los diagnósticos de ruta de acceso EKM en la página 30.

Para activar los diagnósticos automáticos de ruta de acceso EKM:

1. En el cliente web, seleccione **Setup (Configuración) > Encryption (Cifrado) > System Configuration (Configuración del sistema)**.
2. Seleccione la casilla de verificación **Automatic EKM Path Diagnostics (Diagnósticos automáticos de prueba de acceso EKM)**.
3. Seleccione un intervalo en la lista desplegable.
4. Especifique el número de intervalos omitidos de pruebas consecutivas necesarios para que la biblioteca genere un vale de RAS que informe que la prueba no se pudo realizar dentro de los intervalos especificados.

Visualización de la configuración de cifrado de la unidad de cinta

Puede ver la configuración de cifrado de las siguientes maneras:

- **System Information Report (Informe de información del sistema)**: para ver la información de cifrado en la totalidad de servidores de claves, particiones y unidades de cinta, seleccione **Reports (Informes) > System Information (Información del sistema)** en el cliente web. Para obtener más información, consulte la *Guía del usuario de Dell PowerVault ML6000*.
- **Library Configuration Report (Informe de configuración de biblioteca)**: para ver el estado de cifrado de un cartucho de cinta o una unidad de cinta seleccionada, seleccione **Reports (Informes) > Library Configuration (Configuración de biblioteca)** en el cliente web y haga clic en la unidad de cinta o ranura. Aparecerá una ventana emergente que muestra el estado del cifrado. Para obtener más información, consulte la *Guía del usuario de Dell PowerVault ML6000*.
- **Partition Encryption (Cifrado de la partición)**: en el cliente web, seleccione **Setup (Configuración) > Encryption (Cifrado) > Partition Configuration (Configuración de partición)** para ver y cambiar la configuración de cifrado de las particiones. Consulte el Paso 3: Configuración del cifrado de partición en la página 27 para obtener más detalles.

ПРОЧИТАЙТЕ В ПЕРВУЮ ОЧЕРЕДЬ! Установка диспетчера ключей шифрования Dell в библиотеке PowerVault™ ML6000 (Russian)

Предупреждения

ОСТОРОЖНО! Знак «ОСТОРОЖНО!» указывает на возможность повреждения оборудования и потери данных в случае невыполнения инструкций.

Назначение данного документа

Диспетчер ключей шифрования Dell Encryption Key Manager, (EKM) представляет собой приложение для управления ключами, применяемыми для шифрования данных при использовании устройств IBM LTO-4 и IBM LTO-5. Управляемое библиотекой шифрование является необязательной лицензируемой функцией, которая должна быть включена в библиотеке PowerVault ML6000 для шифрования данных с использованием возможностей шифрования стримеров LTO-4/LTO-5.

Приложение Dell EKM представляет собой Java-программу IBM, позволяющую стримерам с функцией шифрования генерировать, защищать, хранить и обслуживать ключи шифрования, используемые для шифрования информации, записываемой на ленточные носители, и для расшифровки информации, считываемой с них. Управление политикой и ключи передаются через интерфейс библиотеки, поэтому шифрование является прозрачным для приложений.

Дополнительную информацию об установке и настройке сервера EKM и рекомендуемых процедурах Dell EKM см. в *Руководстве пользователя Dell PowerVault Encryption Key Manager* и в документе *Рекомендуемые процедуры по работе с Dell Encryption Key Manager и шифрованием библиотеки. Вопросы и ответы*.

ПРИМЕЧАНИЕ. Для правильной работы приложения Dell EKM необходимо обновить встроенное программное обеспечение библиотеки и стримера до последних версий. Последние версии встроенного программного обеспечения и инструкций по установке см. на веб-странице http://support.dell.com.

Поддерживаемые стримеры и носители

Шифрование библиотеки в системе PowerVault ML6000 поддерживает шифрование только картриджей данных LTO-4 и LTO-5 с использованием стримеров IBM LTO-4 и LTO-5 Fibre Channel и SAS. ML6000 не поддерживает шифрование для стримеров других типов и других производителей, даже если они назначены разделу, выбранному для шифрования. Для других типов носителей (например, LTO-3) стримеры с включенным шифрованием обеспечивают только чтение, но не шифрование.

Установка Dell EKM на сервере

Для установки приложения Dell EKM необходим один или несколько серверов. В комплект поставки программного обеспечения для шифрования библиотеки входит компакт-диск с программным обеспечением для установки на сервере, а также инструкции по установке и руководство пользователя. Перед установкой EKM в библиотеке необходимо установить сервер(-ы) EKM и установить ключ лицензии.

ПРИМЕЧАНИЕ. Поскольку при чтении и записи на стример с включенным шифрованием библиотека Dell PowerVault ML6000 должна обмениваться данными с сервером EKM в режиме реального времени, настоятельно рекомендуется использовать как первичный, так и вторичный сервер EKM. В таком случае если первичный сервер будет недоступен в тот момент, когда библиотеке

потребуются данные шифрования, запрос может быть обработан вторичным сервером. Библиотека Dell PowerVault ML6000 позволяет использовать до двух серверов EKM для обеспечения избыточности при обработке отказов.

Настройка шифрования в библиотеке

Шаг 1. Установка лицензионного ключа

ПРИМЕЧАНИЕ. Убедитесь в том, что встроенное программное обеспечение библиотеки и стримера обновлено до последней выпущенной версии. Последние версии встроенного программного обеспечения и инструкций по установке см. на веб-странице www.support.dell.com.

1. Получите лицензионный ключ для шифрования, следуя инструкциям в предоставленном *Сертификате лицензионного ключа*.
2. Выполните одно из следующих действий:
   - На панели оператора выберите **Setup (Настройка) > Licenses (Лицензии)**.
   - В окне веб-клиента выберите **Setup (Настройка) > License (Лицензия)**.
3. Введите новый лицензионный ключ.
4. Нажмите кнопку **Apply (Применить)**.

   Откроется окно хода выполнения с указанием затраченного времени. По окончании выполнения появится сообщение **Success (Успешное выполнение)** зеленого цвета и будет показано состояние «Operation Succeeded» (Операция выполнена успешно). После этого шифрование выводится на экране в списке доступных функций. (Появление сообщения **Failure (Сбой)** может указывать на то, что введен неправильный лицензионный ключ.)
5. Нажмите кнопку **Close (Закрыть)**.

Шаг 2. Настройка параметров шифрования и адресов сервера ключей

1. Извлеките картриджи из всех поддерживающих шифрование стримеров в библиотеке.
2. В окне веб-клиента выберите **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)**.
3. **Automatic EKM Path Diagnostics (Автоматическая диагностика путей EKM)**: включите или выключите эту функцию и установите необходимый интервал проверки. Кроме того, можно указать количество последовательно пропущенных интервалов проверки, после которого генерируется ярлык RAS. Дополнительные сведения см. в разделе Автоматическая диагностика путей EKM на стр. 40.
4. **Secure Sockets Layer (SSL)**: установите флажок **SSL Connection (Соединение SSL)**, чтобы включить SSL для обмена данными между библиотекой и серверами ключей EKM. Значение по умолчанию: «Disabled» (Отключено). При включении SSL необходимо убедиться в том, что **Primary** и **Secondary Key Server Port Numbers (Номера портов первичного и вторичного сервера ключей**, см. ниже) совпадают с номерами портов SSL, установленными на серверах EKM. По умолчанию используется номер порта 443.

ПРИМЕЧАНИЕ. Шифрование ключей выполняется перед каждой отправкой ключей с сервера ключей EKM на стример вне зависимости от того, включен или отключен SSL. Включение SSL позволяет повысить уровень безопасности.

5. В текстовом поле **Primary Key Server IP Address or Host (IP-адрес или хост первичного сервера ключей)** введите одно из следующих значений:
   - IP-адрес первичного сервера ключей (если DNS не включена) или
   - Имя узла первичного сервера ключей (если DNS включена)
6. Введите номер порта первичного сервера ключей в текстовое поле **Primary Key Server Port Number (Номер порта первичного сервера ключей)**. До включения SSL по умолчанию используется номер порта 3801. При включенном SSL по умолчанию используется номер порта 443.

ПРИМЕЧАНИЕ. При изменении настройки номера порта в библиотеке необходимо соответственно изменить и номер порта на сервере ключей, иначе EKM будет работать неправильно.

7 Если для предупреждения сбоев используется вторичный сервер ключей, введите IP-адрес или имя узла вторичного сервера ключей в текстовое поле **Secondary Key Server IP Address or Host (IP-адрес или хост вторичного сервера ключей)**.

ПРИМЕЧАНИЕ. Если использовать вторичный сервер ключей не планируется, в поле **Secondary Key Server IP Address or Host (IP-адрес или хост вторичного сервера ключей)** можно ввести нулевой IP-адрес (0.0.0.0) или оставить это поле пустым.

8 Если в предыдущем пункте настроен вторичный сервер ключей, введите номер порта вторичного сервера ключей в текстовое поле **Secondary Key Server Port Number (Номер порта вторичного сервера ключей)**. Если не включен протокол SSL, по умолчанию используется номер порта 3801. Если включен протокол SSL, по умолчанию используется номер порта 443.

ПРИМЕЧАНИЕ. Если используется вторичный сервер ключей, на обоих серверах (первичном и вторичном) должны быть настроены одинаковые номера портов. Если они будут различаться, синхронизация и обработка отказа будут невозможны.

9 Нажмите кнопку **Apply (Применить)**.

Откроется окно хода выполнения. В нем приведена информация о выполняемом действии, затраченном времени и состоянии выполнения. Выполните одно из следующих действий:

- Если в окне хода выполнения выводится сообщение **Success (Успешное выполнение)**, настройка системы EKM успешно завершена. Нажмите кнопку **Close (Закрыть)**, чтобы закрыть окно выполнения.
- Если в окне хода выполнения выводится сообщение **Failure (Сбой)**, настройка системы EKM не была успешно завершена. Для устранения проблем, возникших в процессе выполнения операции, следуйте указаниям в окне хода выполнения.

ПРИМЕЧАНИЕ. Если для разных разделов планируется использовать разные серверы ключей EKM, необходимо заполнить раздел замен в окне **Setup (Настройка) > Encryption (Шифрование) > Partition Encryption (Шифрование раздела)**. См. раздел Шаг 3. Настройка шифрования раздела.

Шаг 3. Настройка шифрования раздела.

Шифрование в ленточной библиотеке Dell PowerVault ML6000 может быть включено только для определенного раздела. Возможность выбора отдельных стримеров для шифрования не предусмотрена; необходимо выбрать полный раздел для шифрования. Если для какого-либо раздела включено шифрование, все стримеры с поддержкой шифрования в разделе могут использовать шифрование, и все данные, записываемые на носитель с поддержкой шифрования в этом разделе, шифруются. Все стримеры в этом разделе, для которых шифрование не поддерживается, не будут использовать шифрование, и записываемые на неподдерживаемые носители данные не будут шифроваться.

Данные, записываемые на носители, которые поддерживают шифрование и для которых оно включено, расположенные в стримерах с поддержкой шифрования, будут шифроваться, *если* на этот носитель ранее не были записаны данные в незашифрованном формате. Для того чтобы данные шифровались, носитель должен быть пустым либо при первой операции записи в начале ленты данные должны быть записаны с использованием шифрования.

Выполните настройку раздела или разделов следующим образом:

1 В окне веб-клиента выберите **Setup (Настройка) > Encryption (Шифрование) > Partition Configuration (Конфигурация раздела)**.

Откроется список всех разделов с раскрывающимся списком методов шифрования для каждого раздела.

2 При изменении метода шифрования раздела убедитесь, что в стримерах этого раздела нет картриджей. Если в стримерах имеются картриджи, метод шифрования нельзя изменить.

www.dell.com | support.dell.com

3 Выберите в раскрывающемся списке нужный метод шифрования для каждого раздела. (Для стримеров с поддержкой шифрования по умолчанию используется метод **Application Managed (Управляется приложением)**). Выбранный метод шифрования применяется ко всем поддерживающим шифрование стримерам и носителям в этом разделе.

Метод шифрования	Описание
Library Managed (Управляется библиотекой)	**Используется с EKM.** Обеспечивает поддержку шифрования с помощью подключенного сервера ключей Dell EKM для всех стримеров и носителей с поддержкой шифрования, назначенных данному разделу.
Application Managed (Управляется приложением)	**Не используется с EKM.** Позволяет использовать шифрование средствами внешнего приложения резервного копирования для всех стримеров и носителей в данном разделе, поддерживающих шифрование. Библиотека НЕ БУДЕТ осуществлять обмен данными с сервером Dell EKM для этого раздела. Это значение используется по умолчанию, если в данном разделе есть стримеры, поддерживающие шифрование. Этот значение должно оставаться выбранным, *кроме случая*, когда не требуется, чтобы программа Dell EKM управляла шифрованием. **ПРИМЕЧАНИЕ.** Если требуется управление шифрованием средствами какого-либо приложения, необходимо отдельно настроить приложение для выполнения этих функций. Шифрование такого типа осуществляется без использования библиотеки.
None (Нет)	Отключает шифрование раздела.
Unsupported (Не поддерживается)	Означает, что в данном разделе нет стримеров, поддерживающих шифрование. Значение **Unsupported (Не поддерживается)** выводится серым цветом, его невозможно изменить.

4 Если разные разделы должны использовать разные серверы ключей EKM, заполните раздел «Library Managed Encryption Server Overrides» (Замены сервера управляемого библиотекой шифрования), как описано в этом шаге. Параметры раздела замен заменяют параметры по умолчанию, представленные на экране **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)**. Замена не изменяет параметры на экране **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)**. Эти параметры установлены по умолчанию для всех разделов, не использующих замены. Замены доступны только для разделов, для которых задан метод шифрования **Library Managed (Управляется библиотекой)**.

ОСТОРОЖНО! Заполнять раздел замен нужно только в том случае, если разные разделы должны использовать разные серверы ключей EKM. В противном случае не изменяйте параметры этого раздела. Здесь будут установлены значения с экрана **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)**. В случае изменения данных раздела замен значения по умолчанию экрана **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)** не будут применяться. Для восстановления параметров по умолчанию после изменения параметров замены нужно будет настроить эти параметры вручную.

Выполните следующие действия для всех разделов, для которых выбран метод шифрования «Library Managed» (Управляется библиотекой):

- Введите IP-адрес (если не используется DNS) или имя узла (если используется DNS) первичного сервера ключей EKM в текстовое поле **Primary Host (Первичный узел)**.

- Введите номер порта первичного сервера ключей EKM в текстовое поле **Port (Порт)**. Если не включен протокол SSL, по умолчанию используется номер порта 3801. Если включен протокол SSL, по умолчанию используется номер порта 443.
- При использовании вторичного сервера ключей EKM введите адрес или имя узла и номер порта вторичного сервера EKM в текстовые поля **Secondary Host (Вторичный узел)** и **Port (Порт)**.
- Установите флажок **SSL (SSL)**, если нужно включить протокол SSL для обмена данными между этим разделом и серверами EKM. Значение по умолчанию: «Disabled» (Отключено). При включении SSL необходимо убедиться в том, что первичный и вторичный номера портов EKM в разделе замен соответствуют номерам портов SSL, установленным на серверах EKM. По умолчанию используется номер порта 443.

ПРИМЕЧАНИЕ. Шифрование ключей выполняется перед каждой отправкой ключей с сервера EKM на стример вне зависимости от того, включен или отключен SSL. Включение SSL позволяет повысить уровень безопасности.

ПРИМЕЧАНИЕ. Restriction on EKM servers used for overrides (Ограничения на серверах EKM для замен): если первичный и вторичный серверы используются для замен, действует следующее ограничение. Если вторичный сервер не используется, ограничений нет.

Restriction (Ограничение): данные первичный и вторичный серверы должны быть «сдвоенными» и не могут использоваться в других комбинациях. Например:
• Server1 может быть первичным, а Server2 вторичным для некоторых или всех разделов.
• Если Server1 является первичным, а Server2 вторичным в одном из разделов, то во всех остальных разделах, использующих Server1, Server1 может быть только первичным и должен быть «сдвоенным» с Server2 в качестве вторичного. Другие разделы не могут использовать в качестве первичного Server1, а в качестве вторичного — Server3.
• Server1 не может быть одновременно первичным в разделе PartitionA и вторичным в разделе PartitionB.
• Server2 не может быть одновременно вторичным в разделе PartitionA и первичным в разделе PartitionB.

При использовании замен убедитесь, что Dell EKM установлен на всех указанных серверах. После этого запустите ручную диагностику пути EKM на всех стримерах и всех разделах, настроенных для EKM, чтобы убедиться, что каждый стример может обмениваться данными с указанным сервером ключей EKM и получать от него ключи. Дополнительные сведения см. в разделе Использование диагностики путей EKM на стр. 38.

5 Нажмите кнопку **Apply (Применить)**.

Откроется окно хода выполнения. В нем содержится информация о выполняемом действии, затраченном времени и состоянии выполнения операции. Выполните одно из следующих действий:

- Если в окне хода выполнения выводится сообщение **Success (Успешное выполнение)**, настройка системы EKM успешно завершена. Нажмите кнопку **Close (Закрыть)**, чтобы закрыть окно выполнения.
- Если в окне хода выполнения выводится сообщение **Failure (Сбой)**, настройка системы EKM не была успешно завершена. Для устранения проблем, возникших в процессе выполнения операции, следуйте указаниям в окне выполнения.

6 Сохраните конфигурацию библиотеки (инструкции см. в *Руководстве пользователя библиотеки Dell PowerVault ML6000).*

Шаг 4. Запуск диагностики путей EKM

Запустите диагностику путей EKM, чтобы убедиться, что стримеры и серверы ключей подключены и работают правильно. См. раздел Использование диагностики путей EKM на стр. 38.

www.dell.com | support.dell.com

Резервное копирование данных хранилища ключей

Поскольку ключи в хранилище имеют исключительно важное значение, необходимо создавать резервные копии данных хранилища ключей на устройстве, не использующем шифрование, чтобы иметь возможность восстановления этих данных при необходимости и чтения носителей на магнитной ленте, записанных с использованием этих ключей шифрования, связанных с данным стримером или библиотекой.

Использование диагностики путей EKM

Диагностика путей EKM состоит из ряда коротких тестов, позволяющих проверить работу серверов ключей, их подключение и возможность предоставлять ключи так, как требуется.

Запускайте ручную диагностику путей EKM каждый раз после изменения настроек сервера ключей или шифрования библиотеки, а также после замены стримеров. Рекомендуется проверять все устройства, взаимодействующие с серверами ключей.

Диагностика включает следующие проверки:

ПРИМЕЧАНИЕ. Проверяемый стример должен быть выгружен, готов и находиться в рабочем режиме.

- **Ping**: проверка обмена данными между библиотекой и серверами ключей по сети Ethernet. Если раздел выбранного стримера использует замены сервера EKM, то будет выполнена проверка IP-адресов замен (см. **Setup (Настройка) > Encryption (Шифрование) > Partition Configuration (Конфигурация раздела)**). Если замены в этом разделе не используются, будет выполнена проверка IP-адресов по умолчанию (см. **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)**).
- **Drive (Устройство)**: проверка пути к стримеру в библиотеке (передача данных от библиотеки к стримеру и от стримера к стримеру). Для выполнения этой проверки стример должен быть выгружен, готов и подключен. В случае сбоя теста проверки пути и конфигурации не выполняются.
- **Path (Путь)**: проверка запуска служб EKM на серверах ключей. Эта проверка не может выполняться после сбоя проверки устройства.
- **Config (Конфигурация)**: проверка способности серверов ключей обслуживать ключи шифрования. Эта проверка не может выполняться после сбоя проверки устройства.

Если во время какой-либо проверки возникает сбой, следуйте приведенным далее рекомендациям, затем выполните проверку еще раз:

- **Ping Test Failure (Сбои при выполнении проверки Ping [Пинг])**: убедитесь, что узел сервера ключей запущен и доступен библиотеке по сети.
- **Drive Test Failure (Сбои при выполнении проверки Drive [Устройство])**: обратитесь к документации по стримеру и следуйте инструкциям по устранению неисправностей.
- **Path Test Failure (Сбои при выполнении проверки Path [Путь])**: убедитесь, что сервер ключей запущен, а параметры порта и SSL соответствуют параметрам конфигурации библиотеки.
- **Config Test Failure (Сбои при выполнении проверки Config [Конфигурация])**: убедитесь, что сервер EKM настроен на прием данных от стримера, проверка которого выполняется.

Имеется два способа проведения диагностики:

- Использование ручной диагностики путей EKM
- Автоматическая диагностика путей EKM

Ручная диагностика отличается от автоматической следующим образом:

- При ручной диагностике проверяемые разделы отключаются. При автоматической диагностике этого не происходит. Поэтому во время проверки перемещение в стримеры может задерживаться.
- Для выполнения ручной диагностики путей EKM необходимо выбрать один проверяемый стример. Поскольку проверка распространяется только на выбранное устройство, то для проверки всех стримеров необходимо запустить проверку несколько раз (по одному разу для каждого устройства). Для проверки всех серверов необходимо выполнить диагностику один раз для каждого раздела,

для которого включено шифрование (каждая пара серверов соединена с уникальным разделом и стримером). Если стример недоступен (он должен быть выгружен, готов и включен), проверки устройства, пути и конфигурации не выполняются.

- Автоматическая диагностика путей EKM проверяет все подключенные серверы EKM по очереди, а библиотека выбирает стример для использования при каждой проверке. Если выбранный стример недоступен (он должен быть выгружен, готов и включен), библиотека пытается проверить другой стример, подключенный к этому серверу ключей, до тех пор пока не будет обнаружен доступный стример. Если ни один из стримеров, подключенных к данному серверу ключей, недоступен, сервер пропускается и проверка не выполняется. Если сервер пропускается в течение «X» последовательных попыток проверки (число «X» настраивается через веб-клиент), библиотека генерирует ярлык RAS. Если стример остается загруженным в течение длительного времени, возможно, он никогда не будет проверен. Если необходимо проверить определенный стример, воспользуйтесь ручной диагностикой пути EKM. В частности, при замене стримера нужно выполнить диагностику пути EKM вручную.

Использование ручной диагностики путей EKM

1 Откройте экран диагностики путей EKM одним из двух способов:

- Войдите в режим диагностики библиотеки (выберите **Tools (Сервис) > Diagnostics (Диагностика)**), затем выберите **EKM > EKM Path Diagnostics (Диагностика путей EKM)**. Учтите, что при входе в режим диагностики все остальные пользователи с таким же или более низким уровнем привилегий будут отключены, а все разделы будут переведены в автономный режим. После выхода из режима диагностики разделы автоматически будут вновь включены.
- Выберите **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация система)** или **Setup (Настройка) > Encryption (Шифрование) > Partition Configuration (Конфигурация раздела)** и щелкните по ссылке «Click here to run EKM Path Diagnostics» (Щелкните здесь для запуска диагностики путей EKM). Обратите внимание, что выполнение этих действий приведет к временной недоступности раздела выбранного стримера. После завершения проверки раздел будет вновь доступен.

Будет выведен список всех стримеров, которые поддерживают управляемое библиотекой шифрование, а также состояние стримеров и разделы, в которых они располагаются.

2 Выберите стример, который нужно проверить, и нажмите кнопку **Apply (Применить)**. Для выполнения этой проверки стример должен быть выгружен, готов и находиться в рабочем режиме.

Откроется диалоговое окно с предупреждением о временной недоступности выбранного раздела.

3 Нажмите **OK**, чтобы начать диагностику.

Откроется окно хода выполнения. В нем содержится информация о выполняемом действии, затраченном времени и состоянии выполнения операции.

Библиотека выполнит диагностику и покажет результаты всех проверок в окне хода выполнения.

ПРИМЕЧАНИЕ. Диагностика может занять несколько минут.

4 Выполните одно из следующих действий:

- Если в окне хода выполнения появилось сообщение **Completed (Выполнено)**, диагностика завершена. Это не означает отсутствие ошибок, а только свидетельствует о завершении процесса диагностики. Нажмите кнопку **Close (Закрыть)**, чтобы закрыть окно хода выполнения.
- Если в окне хода выполнения появилось сообщение **Failure (Сбой)**, диагностика не выполнена. Для устранения проблем, возникших в процессе выполнения операции, следуйте указаниям в окне выполнения.

www.dell.com | support.dell.com

Автоматическая диагностика путей EKM

Можно настроить библиотеку так, чтобы она автоматически выполняла диагностику путей EKM с заданным интервалом времени. В течение этого интервала библиотека проверяет каждый настроенный сервер ключей. При наличии проблем библиотека генерирует ярлык RAS. По умолчанию эта функция отключена. Интервал проверки по умолчанию составляет четыре часа. Автоматическую диагностику путей EKM рекомендуется оставлять выключенной, если только у вас в сети не происходят регулярные сбои шифрования из-за проблем связи.

ОСТОРОЖНО! Выполнение автоматической диагностики путей EKM может привести к увеличению количества ярлыков RAS, если проверки будут пропускаться из-за недоступности стримеров в течение заданного количества последовательных попыток. Чтобы уменьшить количество ярлыков RAS, можно задать более высокое количество последовательных проверок для генерации ярлыка RAS или настроить библиотеку таким образом, чтобы она никогда не генерировала ярлыки RAS в случае пропуска проверок.

Список проводимых проверок см. в разделе Использование диагностики путей EKM на стр. 38.

Включение автоматической диагностики путей EKM:

1. В окне веб-клиента выберите **Setup (Настройка) > Encryption (Шифрование) > System Configuration (Конфигурация системы)**.
2. Установите флажок **Automatic EKM Path Diagnostics (Автоматическая диагностика путей EKM)**.
3. Выберите в списке интервал.
4. Укажите количество последовательных попыток проверки, при достижении которого будет генерироваться ярлык RAS, информирующий о невозможности проверки.

Просмотр параметров шифрования стримера

Просмотреть параметры шифрования можно одним из следующих способов:

- **System Information Report (Отчет информации о системе)**: для просмотра информации о шифровании на всех серверах ключей, во всех разделах и стримерах выберите в веб-клиенте **Reports (Отчеты) > System Information (Информация о системе)**. Более подробную информацию см. в *Руководстве пользователя Dell PowerVault ML6000*.
- **Library Configuration Report (Отчет о конфигурации библиотеки)**: для просмотра состояния шифрования выбранного стримера или картриджа выберите в веб-клиенте **Reports (Отчеты) > Library Configuration (Конфигурация библиотеки)** и щелкните по нужному стримеру или слоту. Состояние шифрования отображается во всплывающем окне состояния. Более подробную информацию см. в *Руководстве пользователя Dell PowerVault ML6000*.
- **Partition Encryption (Шифрование раздела)**: выберите в веб-клиенте **Setup (Настройка) > Encryption (Шифрование) > Partition Configuration (Конфигурация раздела)**, чтобы просмотреть и изменить параметры шифрования разделов. Дополнительные сведения см. в разделе Шаг 3. Настройка шифрования раздела. на стр. 35.

はじめに『PowerVault™ ML6000 に Dell Encryption Key Manager を設定する方法』（Japanese）をお読みください。

「注意」について

注意：注意は、指示に従わないと、ハードウェアの損傷やデータの消失を招く可能性があることを示します。

本書の目的

Dell Encryption Key Manager (EKM) は、IBM LTO-4 および IBM LTO-5 ドライブベースのデータ暗号化処理の一部として使用される暗号鍵を管理する集中キー マネージャ アプリケーションです。ライブラリ管理下にある暗号化は、オプションのライセンス機能です。LTO-4/LTO-5 テープ ドライブの暗号化機能を使用してデータを暗号化するには、PowerVault ML6000 ライブラリから有効にする必要があります。

Dell EKM は IBM Java ソフトウェア プログラムであり、暗号化対応のテープ ドライブにおいて、テープ メディアから読み書きされる情報の暗号化と復号に使用する暗号鍵の生成、保護、保存、保守を行います。ポリシー管理と鍵はライブラリを介して渡されるため、アプリケーションに対して暗号化は透過的です。

EKM サーバーのインストールおよび設定の詳細、Dell EKM のベストプラクティスについては、『Dell PowerVault Encryption Key Manager ユーザーズガイド』および『Dell Encryption Key Manager およびライブラリ管理下暗号化ベストプラクティスと FAQ』を参照してください。

注：Dell EKM が正常に動作するためには、ライブラリとテープ ドライブ ファームウェアを最新のバージョンにアップグレードする必要があります。最新のファームウェアおよびインストール手順は、 http://support.dell.com **から入手できます。**

対応テープ ドライブとメディア

PowerVault ML6000 のライブラリ管理下の暗号化では、IBM LTO-4/LTO-5 Fibre Channel および SAS テープ ドライブを使用する LTO-4 と LTO-5 データ カートリッジ上の暗号化のみがサポートされています。ML600 ライブラリ管理下の暗号化は、暗号化用に選択されたパーティションに割り当てられている場合でも、他のタイプやメーカー ブランドのテープ ドライブ上の暗号化をサポートしていません。他のメディア タイプ（例：LTO-3）を読み取ることは可能ですが、ライブラリ管理下の暗号化に対応しているテープ ドライブで暗号化することはできません。

Dell EKM のサーバーへのインストール

Dell EKM をインストールするサーバーを用意する必要があります。ライブラリ管理下の暗号化を購入すると、サーバーへのインストールに必要なソフトウェア、インストールガイド、ユーザーズガイドが収録された CD が配布されます。ライブラリで EKM を設定する前に、EKM サーバーを設定し、ライセンス キーをインストールしてください。

注：暗号化対応のテープ ドライブから読み取りまたは書き込む際、Dell PowerVault ML6000 ライブラリは EKM サーバーとリアルタイムで通信する必要があるため、プライマリおよびセカンダリ EKM サーバーの両方を必ず使用することを推奨します。こうすることで、ライブラリで暗号化情報が必要な時にプライマリ サーバーが使用できない場合は、セカンダリ サーバーを使用できます。Dell PowerVault ML6000 ライブラリは、フェールオーバー / 冗長化を行う目的で最大 2 台の EKM サーバーの使用をサポートしています。

ライブラリでの暗号化の設定

ステップ 1：ライセンス キーのインストール

注：ライブラリとテープ ドライブ ファームウェアが最新バージョンにアップグレードされていることをご確認ください。最新のファームウェアおよびインストール手順は、www.support.dell.com をご参照ください。

1 受け取ったライセンス キー証明書に記載されている手順に従って暗号化用のライセンス キーを取得します。

2 次のいずれかを行ってください。
- 操作パネルで Setup（設定）> Licenses（ライセンス）を選択します。
- Web クライアントで、Setup（設定）>License（ライセンス）を選択します。

3 新しいライセンス キーを入力します。

4 Apply（適用）をクリックします。
経過時間を表示する進行状況ウィンドウが表示されます。完了すると、緑色で Success（成功）というメッセージが表示され、ステータスが「Operation Succeeded (操作に成功しました)」に変ります。暗号化が機能として画面に表示されます。(Failure (失敗) というメッセージが表示された場合は、正しくないライセンスキーを入力した可能性があります。)

5 Close (閉じる) をクリックします。

ステップ 2：暗号化および鍵サーバーアドレスの設定

1 ライブラリ内の暗号化可能なすべてのテープ ドライブからテープ カートリッジを取り出します。

2 Web クライアントで、Setup (設定) > Encryption (暗号化) > System Configuration (システム設定) を選択します。

3 Automatic EKM Path Diagnostics（自動 EKM パス診断）：この機能を有効または無効にし、任意のテスト間隔を設定します。RAS チケットを生成するために必要な連続的に失敗したテスト間隔を指定することもできます。詳細については、「47 ページの「 自動 EKM パス診断」をご参照ください。

4 SSL（Secure Sockets Layer）：ライブラリと EKM キー サーバー間の SSL 通信を有効にするには、SSL Connection (SSL 接続) チェックボックスを選択します。デフォルトでは無効に設定されています。SSL を有効にする場合、プライマリおよびセカンダリ キー サーバーのポート番号（下記を参照）が EKM キー サーバーで設定した SSL ポート番号と一致する必要があります。デフォルトの SSL ポート番号は 443 です。

注：SSL が有効または無効にかかわらず、キーは必ず暗号化されてから EKM キー サーバーからテープ ドライブへ送信されます。SSL を有効にするこにより、セキュリティ強化を図ることができます。

5 Primary Key Server IP Address or Host（プライマリ キー サーバー IP アドレスまたはホスト）テキストボックスに、次のいずれかを入力します。
- プライマリ キー サーバーの IP アドレス（DNS が無効な場合）、または
- プライマリ キー サーバーのホスト名（DNS が有効な場合）

6 プライマリ キー サーバーのポート番号を Primary Key Server Port Number（プライマリ キー サーバーポート番号）テキストボックスに入力します。デフォルトのポート番号は 3801 です（ SSL が有効でない場合）。SSL が有効な場合は、デフォルトのポート番号は 443 です。

注：ライブラリでポート番号の設定を変更する場合、EKM が正常に動作するためには、キー サーバーで一致するポート番号に変更する必要があります。**7**フェールオーバー目的でセカンダリ キー サーバーを使用する場合、セカンダリ キー サーバーの IP アドレスまたはホスト名を Secondary Key Server IP Address or Host（セカンダリ キー サーバー IP アドレスまたはホスト）テキストボックスに入力します。

注：セカンダリ キー サーバーを使用しない場合は、Secondary Key Server IP Address or Host（セカンダリ キー サーバー IP アドレスまたはホスト）テキストボックスにゼロ IP アドレス「0.0.0.0」を入力するか、空白のままにしておきます。**8**上記ステップでセカンダリ キー サーバーを設定した場合は、セカンダリ キー サーバーのポート番号を Secondary Key Server Port Number（セカンダリ キー サーバーのポート番号）テキストボックスに入力します。デフォルトのポート番号は 3801 です（ SSL が有効でない場合）。SSL が有効な場合は、デフォルトのポート番号は 443 です。

注：セカンダリ キー サーバーを使用する場合、プライマリとセカンダリ キー サーバーのポート番号は、同じ値に設定にする必要があります。同じでない場合は、同期およびフェールオーバーは実行されません。

9 Apply （適用）をクリックします。

進行状況ウィンドウが表示されます。進行状況ウィンドウには、操作、経過時間、および動作状況に関する情報が表示されます。次のいずれかを行ってください。

- 進行状況ウィンドウに **Success（成功）**というメッセージが表示された場合は、EKM システムが正常に設定されたことになります。進行状況ウィンドウを閉じるには、**Close （閉じる）**をクリックします。
- 進行状況ウィンドウに **Failure（失敗）**というメッセージが表示された場合は、EKM システムが正常に設定されなかったことになります。操作中に発生した問題は、進行状況ウィンドウに表示される指示に従って解決してください。

注：パーティションごとに異なる EKM キー サーバーを使用する場合は、Setup（設定）> Encryption（暗号化）> Partition Encryption（パーティションの暗号化）画面の上書きセクションにも必要事項を入力する必要があります。ステップ 3：パーティション暗号化の設定 をご参照ください。

ステップ 3：パーティション暗号化の設定

PowerVault ML6000 テープ ライブラリの暗号化はパーティションのみで有効になります。個々のテープ ドライブを選択して暗号化することはできません。パーティション全体を選択する必要があります。パーティションでライブラリ管理下の暗号化を有効にする場合、パーティション内のライブラリ管理下の暗号化に対応しているすべてのテープ ドライブで暗号化が有効になり、同パーティション内のライブラリ管理下の暗号化に対応しているメディアへのすべてのデータの書き込みは暗号化されます。パーティション内でライブラリ管理下の暗号化に対応していないテープ ドライブでは、暗号化は無効のままで、非対応メディアへのデータの書き込みは暗号化されません。

ライブラリ管理下の暗号化に対応するテープ ドライブの暗号化可能かつ暗号化対応のメディアに書き込まれたデータは、以前に非暗号化形式でメディアにデータが書き込まれた場合を除き、暗号化されます。データを暗号化するには、メディアが空または BOT の最初の書き込み操作でライブラリ管理下の暗号化を使用して書き込まれている必要があります。

パーティションを設定するには、以下の手順に従います。

1. Web クライアントで、**Setup（設定）> Encryption（暗号化）> Partition Configuration（パーティションの設定）**を選択します。

   すべてのパーティションのリストに、各パーティションの暗号化方法が含まれるドロップダウン リストが含まれて表示されます。
2. パーティションの暗号化方法を変更する場合は、対象のパーティション内のテープ ドライブにカートリッジが入っていないことを確認してください。テープ ドライブにカートリッジが入っている場合、暗号化方法を変更することはできません。
3. 各パーティションに対して、ドロップダウン リストから暗号化方法を選択します。（暗号化に対応しているテープ ドライブの場合、デフォルトは **Application Managed（アプリケーション管理下）**になっています）暗号化方法は、対象パーティション内の暗号化可能なすべてのテープ ドライブおよびメディアに適用されます。

暗号化方法	説明
Library Managed (ライブラリ管理下)	**EKM で使用します。**対象パーティションに割り当てられている暗号化可能なすべてのテープ ドライブとメディアに対して、接続された Dell EKM キー サーバーを介して暗号化サポートを提供します。
Application Managed (アプリケーション管理下)	**EKM で使用しません。**対象パーティション内の暗号化可能なテープ ドライブおよびメディアすべてに対して、外部バックアップ アプリケーションによる暗号化サポートを提供します。ライブラリは、このパーティションの Dell EKM サーバーとは通信しません。 パーティションに暗号化できるテープ ドライブがある場合のデフォルトの設定です。Dell EKM で暗号化を管理する時以外では、このオプションは選択したままの状態にします。 **注：アプリケーションによって暗号化を管理する場合は、そのようにアプリケーションを設定する必要があります。その場合、ライブラリは暗号化に関与しません。**
None (なし)	パーティションで暗号化を無効にします。

www.dell.com | support.dell.com

Unsupported (非対応)	そのパーティション内のテープ ドライブは暗号化できないことを示します。 **Unsupported（非対応）**はグレー表示されており、変更できません。

4 パーティションごとに異なる EKM キー サーバーを使用するには、このステップに記載される Library Managed Encryption Server Overrides（ライブラリ管理下の暗号化サーバーの上書き）のセクションに必要事項を入力します。上書きセクションの設定は、**Setup（設定）> Encryption（暗号化）> System Configuration（システム設定）**画面に表示されるデフォルト設定に優先します。（ただし、上書き設定によって、**Setup（設定）> Encryption （暗号化）> System Configuration（システム設定）**画面に表示された設定は変更されません。これらの設定は、上書きを使用しないパーティションのデフォルト設定です。）上書きを使用できるのは、**Library Managed（管理ライブラリ）**が暗号化方法に設定されたパーティションに限られます。

注意：パーティションごとに異なる EKM キー サーバーを使用する場合にのみ、上書きセクションに必要事項を入力します。そうでない場合は、このセクションはそのままの状態にし、Setup（設定）> Encryption（暗号化）> System Configuration（システム設定）画面に表示された値をこれらのフィールドに入力します。上書きセクションに対して変更を加えると、Setup （設定）> Encryption（暗号化）> System Configuration （システム設定）画面に表示されたデフォルト値は、これらのフィールドに自動的に入力されなくなります。上書きを変更した後でデフォルト設定に戻す場合は、手動で入力する必要があります。

ライブラリ管理下を暗号化方法として使用する各パーティションに対しては、以下の操作を行います。

- プライマリ EKM キー サーバーの IP アドレス（DNS が無効な場合）またはホスト名（DNS が有効な場合）を **Primary Host （プライマリ ホスト）**テキストボックスに入力します。
- プライマリ EKM キー サーバーのポート番号を **Port （ポート）**テキストボックスに入力します。デフォルトのポート番号は 3801 です（ SSL が無効な場合）。SSL が有効な場合は、デフォルトのポート番号は 443 です。
- セカンダリ EKM キー サーバーを使用している場合は、セカンダリ EKM キー サーバーのアドレス / ホスト名およびポート番号を **Secondary Host（セカンダリ ホスト）**および **Port（ポート）**の各テキストボックスに入力します。
- SSL (Secure Sockets Layer) をパーティションと EKM サーバー間の通信に使用するには、**SSL** チェックボックスを選択します。デフォルトでは無効に設定されています。SSL を有効にする場合は、上書きセクションのプライマリおよびセカンダリ EKM ポート番号が EKM サーバー上の SSL ポート番号に一致することを確認してください。デフォルトの SSL ポート番号は 443 です。

注：SSL が有効か無効かに関係なく、キーは必ず暗号化されてから EKM サーバーからテープ ドライブへ送信されます。SSL を有効にするこにより、セキュリティ強化を図ることができます。

注：上書きに使用される EKM サーバーの制限：上書きにプライマリおよびセカンダリ サーバーを使用する場合、次の制限が適用されます。（セカンダリ サーバーを使用しない場合、制限はありません。）

制限：プライマリ サーバーとセカンダリ サーバーは「ペア」になっている必要があり、異なる組み合わせで使用することはできません。例：
- いずれかまたはすべてのパーティションに対して、Server1 にプライマリ、Server2 にセカンダリを使用できます。
- あるパーティションで Server1 がプライマリで Server2 がセカンダリの場合、Server1 を使用するその他のすべてのパーティションでは、Server1 はプライマリになり、セカンダリとして Server2 と「ペア」にする必要があります。別のパーティションで Server1 をプライマリ、Server3 をセカンダリにすることはできません
- Server1 を PartitionA でプライマリにし、PartitionB でセカンダリにすることはできません。
- Server2 を PartitionA でセカンダリにし、PartitionB でプライマリにすることはできません。

上書きを使用する場合は、指定するすべてのサーバー上に Dell EKM をインストールすることを確認します。次に、EKM 用に設定された各パーティションのテープ ドライブ上で手動 EKM パス診断を実行し、各テープ ドライブが指定の EKM キー サーバーと通信し、キーを受け取ることができることを確認します。詳細については、「45 ページの「 EKM パス診断の使用」をご参照ください。

5 Apply**（適用）**をクリックします。

進行状況ウィンドウが開きます。進行状況ウィンドウには、操作、経過時間、および要求された動作の状況に関する情報が表示されます。次のいずれかを行ってください。

- 進行状況ウィンドウに **Success（成功）**というメッセージが表示された場合は、EKM システムが正常に設定されたことになります。進行状況ウィンドウを閉じるには、**Close（閉じる）**をクリックします。

- 進行状況ウィンドウに **Failure（失敗）**というメッセージが表示された場合は、EKM システムが正常に設定されなかったことになります。操作中に発生した問題は、進行状況ウィンドウに表示される指示に従って解決してください。

6 ライブラリの設定を保存します（保存手順は『Dell PowerVault ML6000 ユーザーズガイド』を参照）。

ステップ 4：EKM パス診断の実行

テープ ドライブとキー サーバーが接続され、正しく動作していることを確認するために、EKM パス診断を実行します。45 ページの「 EKM パス診断の使用 をご参照ください。

キーストア データのバックアップ

キーストア内のキーは大変重要であるため、必ず暗号化されていないデバイスにキー ストア データをバックアップしておいてください。こうすることにより、必要に応じて、そのテープ ドライブまたはライブラリに関連付けられている暗号鍵を使用して暗号化されたテープを読み取ることができます。

EKM パス診断の使用

EKM パス診断は、キー サーバーが稼動し、接続され、必要に応じてキーを提供できることを検証する一連の小テストで構成されます。

キー サーバー設定またはライブラリ暗号化設定の変更時、そしてテープ ドライブの交換時には、手動 EKM パス診断を実行します。キー マネージャ サーバーと通信する各ドライブに対して、テストを実行することが推奨されます。

診断は以下のテストから構成されています。

注：いずれのテストを実行する場合も、テストに使用されるテープ ドライブが空で、使用可能な状態にあり、オンラインである必要があります。

- Ping — ライブラリとキー サーバー間のイーサネット通信リンクを検証します。選択したテープ ドライブが存在するパーティションが EKM サーバーの上書きを使用する場合、上書き IP アドレスがテストされます（**Setup（設定）> Encryption（暗号化）> Partition Configuration（パーティションの設定）**を参照）。パーティションが上書きを使用しない場合は、デフォルト システムの IP アドレスがテストされます（**Setup（設定）> Encryption（暗号化）> System Configuration（システム設定）**を参照）。
- **Drive（ドライブ）** — ライブラリ内のテープ ドライブのパスを検証します（ライブラリからテープ ドライブスレッド、およびテープ ドライブスレッドからテープ ドライブへの通信）。このテストを実行するには、テープ ドライブが空で、使用可能な状態にあり、オンラインである必要があります。テストに失敗すると、パスおよび設定テストは実行されません。
- **Path（パス）** — キー サーバー上で EKM サービスが実行されていることを検証します。ドライブ テストが失敗した場合、このテストを実行できません。
- **Config（設定）** — キー サーバーが暗号鍵を提供できることを検証します。ドライブ テストが失敗した場合、このテストを実行できません。

合格しないテストがあった場合は、以下の解決策を試してみた上で、テストを再試行します。

- **Ping Test Failure（Ping テストの失敗）** — キー サーバー ホストが稼動し、ライブラリが接続されるネットワークからアクセス可能かどうかを検証します。
- **Drive Test Failure（ドライブのテストの失敗）** — テープ ドライブ RAS チケットを検索し、チケット内の解決手順に従います。
- **Path Test Failure（パスのテストの失敗）** — キー サーバーが実際に稼動し、ポート /SSL 設定がライブラリ設定と一致することを検証します。
- **Config Test Failure（設定テストの失敗）** — EKM サーバーがテスト中のテープ ドライブを受け取ることができるように設定されているかを検証します。

診断は、次の 2 つの方法で実行できます。

www.dell.com | support.dell.com

- 手動 EKM パス診断
- 自動 EKM パス診断

手動診断は、次のように自動診断とは異なります。

- 手動診断は、対象パーティションをオフラインにします。自動診断は、対象パーティションをオフラインにしません。テスト中は、テープ ドライブの動作に遅延が発生する場合があります。
- 手動 EKM パス診断では、テストに使用するテープ ドライブを 1 つ選択する必要があります。テストは選択されたドライブのみを検証するため、各テープ ドライブのパスをテストする場合、テストを何度も（ドライブごとに 1 回）実行する必要があります。すべてのサーバーをテストするには、ライブラリ管理下の暗号化が有効なパーティションごとに、診断を実行する必要があります（各サーバー ペアは、固有のパーティションとテープ ドライブに接続されます）。テープ ドライブを利用できない場合（空で、使用可能な状態にあり、オンラインである必要があります）、ドライブ、パス、および設定の各種テストは実行されません。
- 自動 EKM パス診断は、接続されているすべての EKM サーバーを順にテストし、各テストに使用するテープ ドライブを選択します。選択されたテープ ドライブを利用できない場合（空で、使用可能な状態にあり、オンラインである必要があります）、ライブラリは利用できるテープ ドライブが見つかるまで、キー サーバーに接続されている別のテープ ドライブを試します。特定のキー サーバーに接続されているテープ ドライブが利用できない場合、このサーバーはスキップされ、テストは実行されません。サーバーが「X」回（ここで、「X」はウェブ クライアントで設定可能）連続してテスト間隔がスキップされると、ライブラリは RAS チケットを生成します。テープ ドライブが長い間、取り付けられたままになっている場合、同ドライブが全くテストされない可能性があります。特定のテープ ドライブをテストする場合、手動 EKM パス診断を使用します。**テープ ドライブを交換する場合は特に、手動 EKM パス診断を実行してください。**

手動 EKM パス診断

1 次のいずれかの方法で EKM パス診断画面にアクセスします。

- ライブラリ診断にアクセス（Tools（ツール）> Diagnostics（診断））し、EKM > EKM Path Diagnostics（EKM パス診断）を選択します。診断にアクセスすると、同等以下の特権を持つ他のユーザーがすべてログオフされ、パーティションはオフラインになります。診断を終了すると、パーティションは自動的にオンラインに戻ります。
- Setup（設定）> Encryption（暗号化）> System Configuration（システム設定）または Setup（設定）> Encryption（暗号化）> Partition Configuration（パーティション設定）を選択し、[Click here to run EKM Path Diagnostics]（EKM パス診断を実行するにはここをクリック）のリンクをクリックします。この操作を行うと、選択したテープドライブが存在するパーティションはオフラインになります。テストが完了すると、パーティションは自動的にオンラインに戻ります。

ライブラリ管理下の暗号化で使用するすべてのテープ ドライブの一覧が、テープ ドライブの状態および各テープ ドライブが存在するパーティションと共に表示されます。

2 診断を行うテープ ドライブを選択し、Apply（適用）をクリックします。このテストを実行するには、テープ ドライブが空で、使用可能な状態にあり、オンラインである必要があります。

選択したパーティションがオンラインになることを通知するダイアログボックスが表示されます。

3 OK をクリックして診断を開始します。

進行状況ウィンドウが開きます。進行状況ウィンドウには、操作、経過時間、および要求された動作の状況に関する情報が表示されます。

ライブラリによって診断が行われ、進行状況ウィンドウには各テストの合否結果が表示されます。

注：診断テストは完了までに数分がかかることがあります。4次のいずれかを行ってください。

- Completed（完了）が進行状況ウィンドウに表示された場合は、診断が実行されたことになります（診断が実行されたことを示すだけであり、必ずしも診断にパスしたことを意味するわけではありません）。進行状況ウィンドウを閉じるには、Close（閉じる）をクリックします。

- Failure（失敗）が進行状況ウィンドウに表示された場合は、診断を実行できなかったことになります。操作中に発生した問題は、進行状況ウィンドウに表示される指示に従って解決してください。

自動 EKM パス診断

選択した間隔でライブラリが EKM パス診断を自動的に実行するようにできます。指定した間隔ごとに、ライブラリは設定されたすべてのキー サーバーをテストします。問題が発生した場合、ライブラリは RAS チケットを生成します。デフォルトでは、この機能は無効になっています。デフォルトのテスト間隔は、4 時間です。暗号化の失敗がネットワーク中断に起因することが多い場合を除き、自動 EKM パス診断を無効にすることが推奨されます。

注意：テープ ドライブが利用不可のため、テストが指定したテスト間隔数を連続的にスキップすると、RAS チケット数の増加につながる場合があります。RAS チケット数を減らすには、RAS チケットが生成されるまでの連続的なテスト間隔数を増やすか、失敗したテスト間隔に対してライブラリが RAS チケットを生成しないように設定することも可能です。

実行されたテストのリストについては、「45 ページの「 EKM パス診断の使用」を参照してください。

自動 EKM パス診断を有効にするには：

1. Web クライアントで、Setup（設定）> Encryption（暗号化）> System Configuration（システム設定）を選択します。
2. Automatic EKM Path Diagnostics（自動 EKM パス診断）チェックボックスを選択します。
3. ドロップダウン リストから間隔を選択します。
4. ライブラリが指定した間隔内にテストを実行できないことを知らせる RAS チケットが生成されるまでに、連続的に失敗する必要のあるテスト間隔数を指定します。

テープ ドライブの暗号化設定の表示

暗号化設定は、次の方法で表示できます。

- System Information Report（システム情報レポート）— すべてのキー サーバー、パーティション、およびテープ ドライブ上の暗号化情報を表示するには、ウェブ クライアントから Reports（レポート）> System Information（システム情報）を選択します。詳細については、『Dell PowerVault ML6000 ユーザーズガイド』を参照してください。
- Library Configuration Report（ライブラリ設定レポート）— 選択したテープ ドライブまたはテープ カートリッジの暗号化状態を表示するには、ウェブ クライアントから Reports（レポート）> Library Configuration（ライブラリ設定）を選択し、テープ ドライブまたはスロットをクリックします。暗号化ステータスがポップアップ ステータス ウィンドウに表示されます。詳細については、『Dell PowerVault ML6000 ユーザーズガイド』を参照してください。
- Partition Encryption（パーティション暗号化）— パーティションの暗号化設定を表示または変更するには、ウェブ クライアントから Setup（設定）> Encryption（暗号化）> Partition Configuration（パーティション設定）を選択します。詳細については、43 ページの「 ステップ 3：パーティション暗号化の設定」を参照してください。

www.dell.com | support.dell.com

이 부분을 먼저 읽으십시오 - PowerVault ™ ML6000 에서 Dell 암호화 키 관리자 설정 방법 (Korean)

주의 정보

주의 : 주의는 따르지 않을 경우 하드웨어 손상 또는 데이터 유실을 일으킬 수 있는 손상을 나타냅니다 .

이 설명서의 목적

Dell 암호화 키 관리자 (EKM) 는 IBM LTO-4 및 IBM LTO-5 드라이브 기반 데이터 암호화 프로세스의 일부분으로 사용된 암호화 키를 관리하는 중앙집중식 키 관리자 응용 프로그램입니다 . 라이브러리 관리 암호화는 LTO-4/LTO-5 테이프 드라이브 암호화 기능을 사용하여 데이터 암호화를 시작하기 위해 PowerVault ML6000 라이브러리에서 활성화해야 하는 선택 사양의 라이센스 기능입니다 .

Dell EKM 은 IBM Java 소프트웨어 프로그램으로 , 테이프 미디어에 쓰여지는 정보를 암호화하고 이 테이프 미디어에서 읽혀지는 정보를 암호 해독하는 데 사용하는 암호화 키를 생성 , 보호 , 저장 및 유지 관리하는 암호화 기능이 사용 가능한 테이프 드라이브를 지원합니다 . 정책 관리 및 키가 라이브러리를 통해 전달되므로 암호화는 응용 프로그램에 투명합니다 .

EKM 서버 설치 및 구성 방법과 Dell EKM 모범 사례에 대한 자세한 내용은 *Dell PowerVault 암호화 키 관리자 사용 설명서*와 *Dell 암호화 키 관리자 및 라이브러리 관리 암호화 모범 사례 및 FAQ* 자료를 참조하십시오 .

주 : Dell EKM 이 제대로 작동하려면 라이브러리 및 테이프 드라이브 펌웨어를 최신 버전으로 업그레이드해야 합니다 . 최신 펌웨어 및 설치 지침은 http://support.dell.com 에서 확인할 수 있습니다 .

지원 테이프 드라이브 및 미디어

PowerVault ML6000 의 라이브러리 관리 암호화는 IBM LTO-4 및 LTO-5 Fibre Channel 과 SAS 테이프 드라이브를 사용한 LTO-4 및 LTO-5 데이터 카트리지에서의 암호화만 지원합니다 . ML6000 라이브러리 관리 암호화를 위해 선택된 파티션에 지정된다 해도 다른 테이프 드라이브 유형이나 다른 제조업체 브랜드에서의 암호화는 지원하지 않습니다 . 다른 미디어 유형 (예 : LTO-3) 을 읽을 수는 있지만 라이브러리 관리 암호화에 대해 활성화된 테이프 드라이브를 통해 암호화되지는 않습니다 .

서버에 Dell EKM 설치

Dell EKM 을 설치할 서버 또는 서버들이 있어야 합니다 . 라이브러리 관리 암호화를 구매할 때 설치 지침 및 사용 설명서와 함께 서버에 설치할 소프트웨어가 들어 있는 CD 가 제공됩니다 . 라이브러리에 EKM 을 설정하기 전에 EKM 서버를 설정하고 라이센스 키를 설치해야 합니다 .

주 : 암호화가 사용 가능한 테이프 드라이브에서 읽거나 쓸 때 Dell PowerVault ML6000 라이브러리는 EKM 서버와 실시간으로 통신해야 하므로 기본 및 보조 EKM 서버 모두를 사용할 것을 강력히 권장합니다 . 그렇게 함으로써 라이브러리에 암호화 정보가 필요할 때 기본 서버를 사용할 수 없을 경우 보조 서버가 요청을 처리할 수 있습니다 . Dell PowerVault ML6000 라이브러리를 사용하면 장애 조치 / 중복성을 목적으로 최대 2 개의 EKM 서버를 사용할 수 있습니다 .

라이브러리에서 암호화 설정

1 단계 : 라이센스 키 설치

주 : 라이브러리 및 테이프 드라이버 펌웨어가 최신 버전으로 업데이트되어 있는지 확인합니다 . 최신 펌웨어 및 설치 지침은 www.dell.com 에서 확인할 수 있습니다 .

1 받은 *라이센스 키 인증서*의 지침에 따라 암호화를 위한 라이센스 키를 얻습니다 .

2 다음 중 하나를 수행하십시오 .

- 작동자 패널에서 Setup(**설정**) > Licenses(**라이센스**) 를 선택합니다 .
- 웹 클라이언트에서 Setup(**설정**) > License(**라이센스**) 를 선택합니다 .

3 새 라이센스 키를 입력합니다 .

4 Apply(**적용**) 을 클릭합니다 .

진행창이 표시되며 , 경과 시간을 나타냅니다 . 완료되면 초록색 Success(**성공**) 메시지가 나타나고 상태가 "Operation Succeeded"(작업 성공) 으로 변경됩니다 . Encryption(암호화) 가 이제 화면에 기능으로 나열됩니다 . (Failure(**실패**) 메시지가 나타난 경우 올바르지 않은 라이센스 키를 입력한 것일 수 있습니다 .)

5 Close(**닫기**) 를 클릭합니다 .

2 단계 : 암호화 설정 및 키 서버 주소 구성

1 라이브러리에서 암호화가 가능한 모든 테이프 드라이브로부터 테이프 카트리지를 언로드합니다 .

2 웹 클라이언트에서 Setup(**설정**) > Encryption(**암호화**) > Partition Configuration(**파티션 구성**) 을 선택합니다 .

3 Automatic EKM Path Diagnostics(**자동 EKM 경로 진단**): 이 기능을 활성화 또는 비활성화하고 원하는 대로 테스트 간격을 설정합니다 . 또한 RAS 티켓을 생성하는 데 필요한 누락된 연속 테스트 간격의 수를 지정할 수도 있습니다 . 자세한 내용은 자동 EKM 경로 진단 - 54 페이지을 참조하십시오 .

4 SSL(Secure Sockets Layer): 라이브러리와 EKM 키 서버 간 통신에 SSL 을 사용하려면 SSL Connection(SSL **연결**) 확인란을 선택합니다 . 기본값은 Disabled(사용 안 함) 입니다 . SSL 을 사용하려면 아래와 같이 **기본** 및 **보조 키 서버 포트 번호**와 EKM 키 서버에 설정된 SSL 포트 번호가 일치해야 합니다 . 기본 SSL 포트 번호는 443 입니다 .

주 : SSL 사용 여부와 관계 없이 키는 EKM 키 서버에서 테이프 드라이브로 전송되기 전에 항상 암호화됩니다 . SSL 을 사용하면 추가 보안이 제공됩니다 .

5 Primary Key Server IP Address or Host(**기본 키 서버 IP 주소 또는 호스트**) 텍스트 상자에 다음 중 하나를 입력합니다 .

- 기본 키 서버의 IP 주소 (DNS 를 사용하지 않는 경우) 또는
- 기본 키 서버의 호스트 이름 (DNS 를 사용하는 경우)

6 Primary Key Server Port Number(**기본 키 서버 포트 번호**) 텍스트 상자에 기본 키 서버의 포트 번호를 입력합니다 . SSL 을 사용하지 않는 경우 기본 포트 번호는 3801 입니다 . SSL 을 사용하는 경우 기본 포트 번호는 443 입니다 .

주 : 라이브러리에서 포트 번호 설정을 변경하는 경우 , 키 서버의 포트 번호 또한 일치하도록 변경해야 합니다 . 그렇지 않으면 EKM 이 제대로 작동하지 않습니다 .

7 장애 조치용으로 보조 키 서버를 사용 중인 경우, Secondary Key Server IP Address or Host(**보조 키 서버 IP 주소 또는 호스트**) 텍스트 상자에 보조 키 서버의 IP 주소 또는 호스트 이름을 입력합니다 .

주 : 보조 EKM 서버를 사용하지 않으려면 **Secondary Key Server IP Address or Host(보조 키 서버 IP 주소 또는 호스트)** 텍스트 상자에 0.0.0.0 과 같이 IP 주소를 영 (0) 으로 입력하거나 이 텍스트 상자를 공란으로 두어도 됩니다 .

8 보조 EKM 서버를 구성했으면 (이전 단계) Secondary Key Server Port Number(**보조 키 서버 포트 번호**) 텍스트 상자에 보조 키 서버의 포트 번호를 입력합니다 . SSL 을 사용하지 않는 경우 기본 포트 번호는 3801 입니다 . SSL 을 사용하는 경우 기본 포트 번호는 443 입니다 .

주 : 보조 키 서버를 사용 중인 경우 , 기본 및 보조 키 서버의 포트 번호를 동일한 값으로 설정해야 합니다 . 그렇지 않으면 동기화 및 장애 조치 기능이 작동하지 않습니다 .

www.dell.com | support.dell.com

9 Apply(**적용**) 을 클릭합니다 .

진행창이 열립니다 . 진행창에는 동작 , 경과 시간 및 작업 상태에 대한 정보가 포함되어 있습니다 . 다음 중 하나를 수행하십시오 .

- Success(**성공**) 이 진행창에 표시되면 EKM 시스템 설정이 성공적으로 구성된 것입니다 . Close(**닫기**) 를 클릭하여 진행창을 닫습니다 .
- Failure(**실패**) 가 진행창에 표시되면 EKM 시스템 설정 구성이 실패한 것입니다 . 진행창에 나열된 지침에 따라 작업 중에 발생된 모든 문제를 해결합니다 .

주 : 파티션별로 다른 EKM 키 서버를 사용하려면 **Setup(설정) > Encryption(암호화) > Partition Encryption (파티션 암호화)** 화면의 재설정 부분도 작성해야 합니다 . **3** 단계 : 파티션 암호화 구성을 참조하십시오 .

3 단계 : 파티션 암호화 구성

Dell PowerVault ML6000 테이프 라이브러리에서 암호화는 파티션별로만 사용 가능합니다 . 암호화에 개별 테이프 드라이브를 선택할 수 없으며 암호화할 전체 파티션을 선택해야 합니다 . 라이브러리 관리 암호화에 파티션을 사용하고 해당 파티션에 있는 모든 라이브러리 관리 암호화 지원 테이프 드라이브가 암호화에 사용되는 경우 , 파티션의 라이브러리 관리 암호화 지원 미디어에 기록된 모든 데이터가 암호화됩니다 . 해당 파티션에서 라이브러리 관리 암호화에 의해 지원되지 않는 모든 테이프 드라이브는 암호화에 사용되지 않으며 , 비지원 미디어에 기록된 데이터는 암호화되지 않습니다 .

라이브러리 관리 암호화 지원 테이프 드라이브의 암호화 지원 및 암호화 가능 미디어에 기록된 데이터는 이전에 해당 데이터가 비암호화 형식의 미디어에 기록되지 *않은 한* 암호화됩니다 . 데이터를 암호화하려면 미디어가 비어 있거나 테이프 시작점 (BOT) 에 처음 쓰기 작업을 수행할 때 라이브 관리 암호화를 사용하여 기록된 것이어야 합니다 .

다음과 같이 파티션을 구성합니다 .

1 웹 클라이언트에서 Setup(**설정**) > Encryption(**암호화**) > Partition Configuration(**파티션 구성**) 을 선택합니다 .

각 파티션에 대한 암호화 방법을 보여주는 드롭다운 목록과 함께 모든 파티션 목록이 표시됩니다 .

2 파티션의 암호화 방법을 변경하려면 해당 파티션의 테이프 드라이브에 카트리지가 로드되어 있지 않은지 확인합니다 . 테이프 드라이브에 카트리지가 로드되어 있으면 암호화 방법을 변경할 수 없습니다 .

3 드롭다운 목록에서 각 파티션에 대한 암호화 방법을 선택합니다 . (암호화를 지원하는 테이프 드라이브의 경우 기본값은 Application Managed(**응용 프로그램 관리**) 입니다 .) 암호화 방법은 모든 암호화 가능 테이프 드라이브와 해당 파티션에 있는 미디어에 적용됩니다 .

암호화 방법	설명
Library Managed (라이브러리 관리)	**EKM 을 사용하는 경우** . 파티션에 할당된 모든 암호화 가능 테이프 드라이브 및 미디어의 경우 연결된 Dell EKM 키 서버를 통해 암호화 지원을 사용할 수 있습니다 .
Application Managed (응용 프로그램 관리)	**EKM 을 사용하지 않는 경우** . 외부 백업 응용 프로그램에서 파티션의 모든 암호화 가능 테이프 드라이브 및 미디어에 암호화 지원을 제공할 수 있습니다 . 라이브러리는 이 파티션의 Dell EKM 서버와 통신하지 않습니다 . 파티션에 암호화 가능 테이프 드라이브가 있다면 이것이 기본 설정입니다 . Dell EKM 에서 암호화를 관리하지 *않으려면* 이 옵션을 선택된 상태로 두어야 합니다 . **주 :** 응용 프로그램이 암호화를 관리하게 하려면 응용 프로그램을 특별히 구성하여 응용 프로그램이 암호화를 관리하게 할 수 있습니다 . 라이브러리는 이 유형의 암호화 수행에 관여하지 않습니다 .
None(없음)	파티션에 암호화를 사용하지 않습니다 .

Unsupported (지원하지 않음)	파티션에 암호화를 지원하는 테이프 드라이브가 없음을 의미합니다 .
	Unsupported(**지원하지 않음**) 이 표시된 경우 비활성으로 표시되며 설정을 변경할 수 없습니다 .

4 파티션별로 다른 EKM 키 서버를 사용하려면 이 단계의 설명과 같이 Library Managed Encryption Server Overrides(라이브러리 관리 암호화 서버 설정 무시) 부분을 작성합니다 . 무시 부분의 설정은 **Setup(설정) > Encryption(암호화) > System Configuration(시스템 구성)** 화면에 나열된 기본 설정보다 우선합니다 . (그러나 설정 무시는 **Setup(설정) > Encryption(암호화) > System Configuration(시스템 구성)** 화면에 나열된 설정을 변경하지 않습니다 . 이 설정은 설정 무시를 사용하지 않는 모든 파티션의 기본 구성 설정입니다 .) 설정 무시는 암호화 방법이 **Library Managed(라이브러리 관리)** 로 설정된 파티션에 대해서만 적용됩니다 .

주의 : 파티션별로 다른 EKM 키 서버를 사용하려는 경우에만 설정 무시 부분을 작성하십시오 . 그렇지 않으면 이 필드가 Setup(설정) > Encryption(암호화) > System Configuration(시스템 구성) 화면의 값으로 채워지도록 이 부분을 그대로 두십시오 . 설정 무시 부분을 변경하면 이 필드는 더 이상 자동으로 Setup(설정) > Encryption (암호화) > System Configuration(시스템 구성) 화면의 기본값으로 채워지지 않습니다 . 재설정을 변경한 후 기본 설정을 복구하려면 기본 설정을 수동으로 입력해야 합니다 .

암호화 방법이 Library Managed(라이브러리 관리) 인 각 파티션에 대해 다음을 수행합니다 .

- DNS 를 사용하지 않는 경우 **Primary Host(기본 호스트)** 텍스트 상자에 IP 주소를 입력하고 DNS 를 사용하는 경우에는 기본 EKM 키 서버의 호스트 이름을 입력합니다 .
- **Port(포트)** 텍스트 상자에 기본 EKM 키 서버의 포트 번호를 입력합니다 . SSL 을 사용하지 않는 경우 기본 포트 번호는 3801 입니다 . SSL 을 사용하는 경우 기본 포트 번호는 443 입니다 .
- 보조 EKM 서버를 사용하는 경우 **Secondary Host:Port(보조 호스트 : 포트)** 텍스트 상자에 보조 EKM 키 서버의 주소 / 호스트 이름 및 포트 번호를 입력합니다 .
- 해당 파티션과 EKM 서버 간 통신에 SSL(Secure Sockets Layer) 을 사용하려면 **SSL** 확인란을 선택합니다 . 기본값은 Disabled(사용 안 함) 입니다 . SSL 을 사용하려면 재설정 부분의 기본 및 보조 EKM 포트 번호와 EKM 서버에 설정된 SSL 포트 번호가 일치해야 합니다 . 기본 SSL 포트 번호는 443 입니다 .

주 : SSL 사용 여부와 관계 없이 키는 EKM 서버에서 테이프 드라이브로 전송되기 전에 항상 암호화됩니다 . SSL 을 사용하면 추가 보안이 제공됩니다 .

주 : 무시에 사용되는 EKM 서버에 대한 제한 : 무시를 위해 기본 및 보조 서버를 사용 중인 경우 다음의 제한이 적용됩니다 . (보조 서버를 사용하지 않는 경우에는 제한이 없습니다 .)

제한 : 주어진 기본 서버와 보조 서버가 " 쌍을 이루어야 (연결)" 하며 다른 조합으로는 사용할 수 없습니다 . 예 :

- 일부 또는 전체 파티션에 대해 Server1 을 기본 서버로 , Server2 를 보조 서버로 사용할 수 있습니다 .
- 한 파티션에서 Server1 이 기본 서버이고 Server2 가 보조 서버이며 , 다른 모든 파티션에서 Server1 을 사용하는 경우 Server1 은 기본 서버만 될 수 있고 Server2 를 보조 서버로 " 연결 " 해야 합니다 . 다른 파티션에서 Server1 을 기본 서버로 , Server3 을 보조 서버로 사용할 수 없습니다 .
- Server1 을 파티션 A 에서는 기본 서버로 , 파티션 B 에서는 보조 서버로 지정할 수 없습니다 .
- Server2 를 파티션 A 에서는 보조 서버로 , 파티션 B 에서는 기본 서버로 지정할 수 없습니다 .

설정 무시를 사용하려면 지정한 모든 서버에 Dell EKM 을 설치해야 합니다 . 그런 다음 EKM 을 사용하도록 구성된 모든 파티션의 각 테이프 드라이브에 대해 Manual EKM Path Diagnostics(수동 EKM 경로 진단) 를 실행하여 각 테이프 드라이브가 지정된 EKM 키 서버와 통신하고 해당 서버로부터 키를 받을 수 있도록 해야 합니다 . 자세한 내용은 EKM 경로 진단 사용 - 52 페이지을 참조하십시오 .

www.dell.com | support.dell.com

5 Apply(**적용**) 을 클릭합니다 .

진행창이 열립니다 . 진행창에는 동작 , 경과 시간 및 요청 작업 상태에 대한 정보가 포함되어 있습니다 . 다음 중 하나를 수행하십시오 .

- Success(**성공**) 이 진행창에 표시되면 EKM 시스템 설정이 성공적으로 구성된 것입니다 . Close(**닫기**) 를 클릭하여 진행창을 닫습니다 .
- Failure(**실패**) 가 진행창에 표시되면 EKM 시스템 설정 구성이 실패한 것입니다 . 진행창에 나열된 지침에 따라 작업 중에 발생된 모든 문제를 해결합니다 .

6 라이브러리 구성을 저장합니다 (지침은 *Dell PowerVault ML6000 사용 설명서* 참조).

4 단계 : EKM 경로 진단 실행

테이프 드라이브와 키 서버가 연결되고 제대로 실행 중인지 확인하려면 EKM Path Diagnostics(EKM 경로 진단) 를 실행합니다 . EKM 경로 진단 사용 - 52 페이지을 참조하십시오 .

Backing Up Keystore Data(키스토어 데이터 백업)

키스토어에 있는 키의 중요한 특성으로 인해 필요할 때 키스토어 데이터를 복구하고 테이프 드라이브 또는 라이브러리와 연관된 해당 암호화 키를 사용하여 암호화된 테이프를 읽을 수 있도록 비 암호화 장치에 키스토어 데이터를 백업해야 합니다 .

EKM 경로 진단 사용

EKM Path Diagnostics(EKM 경로 진단) 는 키 서버가 실행 중이고 연결되었으며 필요할 때 키 역할을 수행할 수 있음을 확인하기 위한 일련의 간단한 테스트로 구성됩니다 .

키 서버 설정 또는 라이브러리 암호화 설정을 변경하거나 테이프 드라이브를 교체할 때마다 Manual EKM Path Diagnostics(수동 EKM 경로 진단) 를 실행합니다 . 키 관리자 서버와 통신하는 각 드라이브를 테스트하는 것이 권장됩니다 .

진단은 다음과 같은 테스트로 구성됩니다 .

주 : 모든 종류의 테스트를 실행하려면 테스트에 사용된 테이프 드라이브를 언로드해서 준비한 다음 온라인으로 설정해야 합니다 .

- Ping - 라이브러리와 키 서버 간 이더넷 통신을 확인합니다 . 선택한 테이프 드라이브의 파티션이 EKM 서버 설정 무시를 사용하면 설정 무시 IP 주소를 테스트합니다 (Setup(**설정**) > Encryption (**암호화**) > Partition Configuration(**파티션 구성**) 참조). 파티션이 설정 무시를 사용하지 않으면 기본 시스템 IP 주소를 테스트합니다 (Setup(**설정**) > Encryption(**암호화**) > System Configuration(**시스템 구성**) 참조).
- Drive(**드라이브**) - 라이브러리의 테이프 드라이브 경로를 확인합니다 (라이브러리에서 테이프 드라이브 슬레드로의 통신 및 테이프 드라이브 슬레드에서 테이프 드라이브로의 통신). 이 테스트를 실행하려면 테이프 드라이브를 언로드해서 준비한 다음 온라인으로 설정해야 합니다 . 이 테스트가 실패하면 Path(경로) 및 Config(구성) 테스트가 수행되지 않습니다 .
- Path(**경로**) - EKM 서비스가 키 서버에 실행 중인지 확인합니다 . Drive(드라이브) 테스트가 실패한 경우 이 테스트를 실행할 수 없습니다 .
- Config(**구성**) - 키 서버가 암호화 키로 작동할 수 있는지를 확인합니다 . Drive(드라이브) 테스트가 실패한 경우 이 테스트를 실행할 수 없습니다 .

테스트가 실패하면 다음 해결방법을 사용한 후 해당 테스트를 다시 실행하여 통과하도록 합니다 .

- Ping Test Failure(Ping **테스트 실패**) - 키 서버 호스트가 실행 중이고 라이브러리가 연결된 네트워크로부터 액세스할 수 있는지 확인합니다 .
- Drive Test Failure(**드라이브 테스트 실패**) - 모든 테이프 드라이브 RAS 티켓을 검색한 다음 해당 티켓의 해결 지침을 따릅니다 .

- **Path Test Failure(경로 테스트 실패)** - 키 서버가 실제로 실행 중이고 포트 /SSL 설정이 라이브러리 구성 설정과 일치하는지 확인합니다 .
- **Config Test Failure(구성 테스트 실패)** - 테스트 중인 테이프 드라이브를 수락하도록 EKM 서버가 설정되어 있는지 확인합니다 .

진단을 수행하는 방법은 두 가지가 있습니다 .

- 수동 EKM 경로 진단
- 자동 EKM 경로 진단

Manual(수동) 진단은 다음과 같은 점에서 Automatic(자동) 진단과 차이가 있습니다 .

- Manual(수동) 진단은 영향을 받는 파티션을 오프라인 상태로 설정합니다 . Automatic(자동) 진단의 경우에는 파티션을 오프라인으로 설정하지 않습니다 . 따라서 테스트 동안 테이프 드라이브로의 이동이 지연될 수 있습니다 .
- Manual EKM Path Diagnostics(수동 EKM 경로 진단) 를 수행하려면 테스트에 사용할 하나의 테이프 드라이브를 선택해야 합니다 . 이 테스트는 선택한 드라이브만을 확인하므로 각 테이프 드라이브에 대한 경로를 테스트하려면 여러 번 테스트를 실행해야 합니다 (각 드라이브에 대해 한 번씩). 모든 서버를 테스트하려면 각 Library Managed Encryption(라이브러리 관리 암호화) 활성 파티션에 대해 진단을 실행해야 합니다 (각 서버 쌍이 고유한 파티션과 테이프 드라이브에 연결됨). 테이프 드라이브를 사용할 수 없는 경우 (언로드해서 준비한 후 온라인으로 설정해야 함), Drive(드라이브), Path(경로) 및 Config(구성) 테스트가 수행되지 않습니다 .
- Automatic EKM Path Diagnostics(자동 EKM 경로 진단) 는 연결된 모든 EKM 서버를 차례로 테스트하고 라이브러리가 각 테스트에 사용할 테이프 드라이브를 선택합니다 . 선택한 테이프 드라이브를 사용할 수 없는 경우 (언로드해서 준비한 후 온라인으로 설정해야 함), 라이브러리가 사용 가능한 드라이브를 찾을 때까지 키 서버에 연결된 다른 테이프 드라이브를 계속 시도합니다 . 특정 키 서버에 연결된 테이프 드라이브 중 사용 가능한 드라이브가 없는 경우 , 해당 서버를 건너뛰고 테스트가 수행되지 않습니다 . 연속 테스트 간격에 지정된 "X" 수만큼 서버를 건너뛴 경우 라이브러리가 RAS 티켓을 생성합니다 . 테이프 드라이브가 장시간 로드된 상태로 남아 있을 경우 테스트가 불가능할 수 있습니다 . 이 경우 특정 테이프 드라이브를 테스트하려면 Manual EKM Path Diagnostics(수동 EKM 경로 진단) 를 사용해야 합니다 . **특히 , 테이프 드라이브를 교체한 경우 Manual EKM(수동 EKM) 경로 진단을 사용하십시오 .**

수동 EKM 경로 진단

1. 다음 두 가지 방법 중 하나로 EKM Path Diagnostics(EKM 경로 진단) 화면에 액세스합니다 .
   - 라이브러리 진단으로 들어간 다음 (**Tools(도구) > Diagnostics(진단)** 선택) **EKM > EKM Path Diagnostics(EKM 경로 진단)** 를 선택합니다 . Diagnostics(진단) 에 들어가면 동일 권한을 갖고 있거나 권한이 더 적은 다른 모든 사용자가 로그오프되고 파티션이 오프라인 상태로 설정됩니다 . Diagnostics(진단) 를 종료하면 파티션이 자동으로 온라인 상태로 복구됩니다 .
   - **Setup(설정) > Encryption(암호화) > System Configuration(시스템 구성)** 또는 **Setup(설정) > Encryption(암호화) > Partition Configuration(파티션 구성)** 을 선택하고 "Click here to run EKM Path Diagnostics." (EKM Path Diagnostics(EKM 경로 진단) 를 실행하려면 여기를 클릭하십시오 .) 라고 표시된 링크를 클릭합니다 . 이 작업을 수행하면 선택한 테이프 드라이브에 상주하는 파티션이 오프라인으로 설정됩니다 . 그러나 테스트가 완료되면 자동으로 해당 파티션이 온라인으로 다시 설정됩니다 .

   라이브러리 관리 암호화를 사용하는 모든 테이프 드라이브의 목록이 테이프 드라이브 상태 및 각 테이프 드라이브의 파티션과 함께 표시됩니다 .
2. 진단을 수행할 테이프 드라이브를 선택한 다음 **Apply(적용)**를 클릭합니다 . 테스트를 실행하려면 테이프 드라이브를 언로드해서 준비한 다음 온라인으로 설정해야 합니다 .

   선택한 파티션이 오프라인으로 설정된다는 대화상자가 나타납니다 .
3. **OK(확인)** 을 클릭하여 진단을 시작합니다 .

www.dell.com | support.dell.com

진행창이 열립니다 . 진행창에는 동작 , 경과 시간 및 요청 작업 상태에 대한 정보가 포함되어 있습니다 .

라이브러리는 진단을 수행한 다음 Progress(진행) 창에 각 테스트에 대한 통과 / 실패 결과를 표시합니다 .

주 : 진단 테스트를 완료하는 데 몇 분이 소요됩니다 .

4 다음 중 하나를 수행하십시오 .

- Progress(진행) 창에 **Completed(완료)** 가 표시되면 진단이 수행된 것입니다 (이는 진단만 수행되었다는 것이지 해당 진단이 통과되었다는 것이 아님). **Close(닫기)** 를 클릭하여 진행창을 닫습니다 .
- Progress(진행) 창에 **Failure(실패)** 가 표시되면 해당 진단을 수행할 수 없다는 것입니다 . 진행창에 나열된 지침에 따라 작업 중에 발생된 모든 문제를 해결합니다 .

자동 EKM 경로 진단

라이브러리를 사용하여 선택한 간격으로 EKM Path Diagnostics(EKM 경로 진단) 를 자동으로 수행할 수 있습니다 . 각 간격 동안 라이브러리가 각각의 구성된 키 서버를 테스트합니다 . 문제가 발생한 경우 라이브러리가 RAS 티켓을 생성합니다 . 기본적으로 이 기능은 해제되어 있습니다 . 기본 테스트 간격은 4 시간입니다 . 사이트에서 네트워크 중단이 일반적인 암호화 실패 원인이 아닌 이상 Automatic EKM Path Diagnostics(자동 EKM 경로 진단) 를 비활성화하는 것이 좋습니다 .

주의 : Automatic EKM Path Diagnostics(자동 EKM 경로 진단) 을 실행할 때 테이프 드라이브를 사용할 수 없는 이유로 연속 테스트 간격으로 구성된 수만큼 테스트를 건너뛴 경우 RAS 티켓 생성 수가 증가할 수 있습니다 . RAS 티켓 발생을 줄이기 위해 RAS 티켓을 생성하는 데 필요한 연속 테스트 간격의 수를 더 큰 수로 지정하거나 라이브러리에서 누락된 테스트 간격에 대한 RAS 티켓을 생성하지 않도록 설정할 수 있습니다 .

수행된 테스트 목록에 대해서는 EKM 경로 진단 사용 - 52 페이지을 참조하십시오 .

Automatic EKM Path Diagnostics(자동 EKM 경로 진단) 을 사용하려면 :

1 웹 클라이언트에서 **Setup(설정) > Encryption(암호화) > Partition Configuration(파티션 구성)** 을 선택합니다 .

2 **Automatic EKM Path Diagnostics(자동 EKM 경로 진단)** 확인란을 선택합니다 .

3 드롭다운 목록에서 간격을 선택합니다 .

4 라이브러리가 지정된 간격 내에 테스트를 수행할 수 없음을 알려주는 RAS 티켓을 생성하기 전에 필요한 연속 누락 테스트 간격 수를 지정합니다 .

테이프 드라이브 암호화 설정 보기

다음 방법으로 암호화 설정을 확인할 수 있습니다 .

- **System Information Report(시스템 정보 보고서)** - 모든 키 서버 , 파티션 및 테이프 드라이브에 대한 암호화 정보를 보려면 웹 클라이언트에서 **Reports(보고서) > System Information(시스템 정보)** 를 선택합니다 . 자세한 내용은 *Dell PowerVault ML6000 사용 설명서*를 참조하십시오 .
- **Library Configuration Report(라이브러리 구성 보고서)** - 선택한 테이프 드라이브 또는 테이프 카트리지의 암호화 상태를 보려면 웹 클라이언트에서 **Reports(보고서) > Library Configuration(라이브러리 구성)** 을 선택한 다음 , 테이프 드라이브 또는 슬롯을 클릭합니다 . 암호화 상태가 팝업 상태 창에 표시됩니다 . 자세한 내용은 *Dell PowerVault ML6000 사용 설명서*를 참조하십시오 .
- **Partition Encryption(파티션 암호화)** - 파티션의 암호화 설정을 보고 변경하려면 웹 클라이언트에서 **Setup(설정) > Encryption(암호화) > Partition Configuration(파티션 구성)** 을 선택합니다 . 자세한 내용은 3 단계 : 파티션 암호화 구성 - 50 페이지을 참조하십시오 .

请先阅读 - 《How To Set Up Dell Encryption Key Manager On Your PowerVault™ ML6000（如何在 PowerVault™ ML6000 上设置 Dell Encryption Key Manager）》（Simplified Chinese）

关于警告

警告：警告表示如不按说明操作，可能会硬件损坏或数据丢失。

本文档的目的

Dell Encryption Key Manager (EKM) 是一种中央密匙管理器应用程序，可管理作为 IBM LTO-4 和 IBM LTO-5 基于磁带机数据加密过程的一部分的加密密匙。库存机管理加密是一种已获授权的可选功能，该功能必须从 PowerVault ML6000 库存机启用，以便使用 LTO-4/LTO-5 磁带机加密功能开始对数据进行加密。

Dell EKM 是一个 IBM Java 软件程序，它能够帮助启用加密的磁带机生成、保护、存储并维护用于加密写入磁带介质的信息和解密从磁带介质中读取信息的加密密钥。由于策略控制和密匙经过库存机，因此应用程序可以“看到”加密。

有关安装和配置 EKM 服务器和 Dell EKM 最佳做法的更多信息，请参阅 《*Dell PowerVault Encryption Key Manager 用户指南*》和 《*Dell Encryption Key Manager 和库存机管理加密最佳做法与常见问题解答一览表*》。

注意：为使 Dell EKM 能够正常工作，您必须将库存机和磁带机固件升级至最新发布版本。以下网址提供最新的固件和安装说明：http://support.dell.com。

支持的磁带机和介质

PowerVault ML6000 的库存机管理加密功能仅在使用 IBM LTO-4 和 LTO-5 光纤通道和 SAS 磁带机的 LTO-4 和 LTO-5 数据磁带上支持加密。ML6000 库存机管理加密在其他类型磁带机或制造商品牌产品时不支持加密，即使将它们分配到一个为加密而选择的分区也不支持加密。其他介质类型（例如， LTO-3）可以被启用库存机管理加密功能的磁带机读取，但不能进行加密。

在服务器上安装 Dell EKM

您必须提供一个或多个用来安装 Dell EKM 的服务器。您购买库存机管理加密时，就可获得一张 CD，里面包含用于在服务器上安装的软件，以及安装说明和用户指南。您必须先安装 EKM 服务器和安装许可证密钥，才能在库存机上安装 EKM。

注意：由于 Dell PowerVault ML6000 库存机在启用加密的磁带机中读取或写入数据时需要与 EKM 服务器实时通信，强烈建议您同时使用第一和第二 EKM 服务器。使用这种方法，如果在库存机需要加密信息时第一服务器不可用，则可由第二服务器处理请求。Dell PowerVault ML6000 库存机允许您出于故障转移 / 冗余的目的使用最多两个服务器。

在库存机上设置加密

步骤 1：安装许可证密钥

注意：请确保库存机和磁带机固件都已更新至最新发布版本。最新固件和安装说明可从 www.support.dell.com 获得。

1 要获取用于加密的许可证密钥，请按照随附的*许可证密钥证书*的说明操作。

2 执行以下操作之一：
- 从 “operator panel”（操作员面板），选择 “Setup”（安装）> “Licenses”（许可证）。
- 从 “Web client”（Web 客户端），选择 “Setup”（安装）> “License”（许可证）。

3 输入新的许可证密钥。

4 单击 “Apply”（应用）。

随即将出现进度窗口，显示已用时间。完成时，将出现绿色的 “Success”（成功）消息，并且状态将变为 “Operation Succeeded”（操作已成功）。加密现在作为一项功能列在屏幕中。（如果出现 “Failure”（错误）消息，则表示您可能输入了错误的许可证密钥。）

5 单击 “Close”（关闭）。

步骤 2：配置加密设置和密钥服务器地址

1 从库存机里中的所有可加密磁带机上取出磁带盒。

2 从 Web 客户端，选择 “Setup”（安装）> “Encryption”（加密）> “System Configuration”（系统配置）。

3 Automatic EKM Path Diagnostics （自动 EKM 路径诊断）：启用或禁用这个功能，并根据需要设置测试时间间隔。您也可以具体指定生成 RAS 票证所需的连续忽略测试时间间隔次数。有关详细信息，请参阅 " 自动 EKM 路径诊断 "，位于第 60 页。

4 安全套接字层 (SSL)：要启用 SSL 以便库存机和 EKM 密匙服务器进行通信，请选择 “SSL Connection”（SSL 连接）复选框。默认值为 “Disabled”（禁用）。如果您启用了 SSL，您必须确保第一和第二密匙服务器端口号 （见下文）与 EKM 密匙服务器上的 SSL 端口号匹配。默认 SSL 端口号是 443。

注意：无论是否启用 SSL，密匙始终在从 EKM 密匙服务器发送到磁带机之前进行加密。启用 SSL 可进一步增强安全性。

5 在 Primary Key Server IP Address or Host （第一密匙服务器 IP 地址或主机）文本框中，输入以下项之一：
- 第一密匙服务器的 IP 地址 （ DNS 未用），或
- 第一密匙服务器的主机名 （ DNS 启用）。

6 在 Primary Key Server Port Number （第一密匙服务器端口号）文本框中输入第一密匙服务器的端口号。如果没有启用 SSL，则默认端口号是 3801。如果启用 SSL，则默认端口号是 443。

注意：如果您更改库存机的端口号设置，您也必须相应地更改密匙服务器的端口号，否则 EKM 将无法正常工作。

7 如果您出于故障转移的目的使用第二密匙服务器，则在 Secondary Key Server IP Address or Host （第二密匙服务器 IP 地址或主机）文本框中输入第二密匙服务器的 IP 地址或主机名。

注意：如果您不打算使用第二密匙服务器，您可在 Secondary Key Server IP Address or Host（第二密匙服务器 IP 地址或主机名）文本框中输入零 IP 地址，即 0.0.0.0，或者留空不填。

8 如果您配置了第二密匙服务器 （前一步骤），请在 Secondary Key Server Port Number （第二密匙服务器端口号）文本框中输入第二密匙服务器的端口号。如果没有启用 SSL，则默认端口号是 3801。如果启用 SSL，则默认端口号是 443。

注意：如果您要使用第二密匙服务器，则第一和第二密匙服务器的端口号必须设为同一值。如果不设为同一值，将不会执行同步和故障转移。

9 单击 “Apply”（应用）。

随即将打开 Progress Window （进度窗口）。“Progress Window”（进度窗口）包含有关操作、已用时间和操作状态的信息。执行以下操作之一：
- 如果在 “Progress Window”（进度窗口）中出现 “Success”（成功），则表示已成功配置 EKM 系统设置。单击 “Close”（关闭）关闭 “Progress Window”（进度窗口）。
- 如果在 “Progress Window”（进度窗口）中出现 “Failure”（失败），则表示未成功配置 EKM 系统设置。按照 “Progress Window”（进度窗口）中列出的说明解决操作过程中出现的问题。

注意：如果您打算对不同的分区使用不同的 EKM 密匙服务器，您也必须填写 “Setup”（**设置**）> “Encryption”（**加密**）> “Partition Encryption”（**分区加密**）屏幕上的覆盖部分。请参阅 步骤 3：配置分区加密。

步骤 3：配置分区加密

仅能按分区对 Dell PowerVault ML6000 磁带库存机进行加密。不能选择加密单独的磁带机；必须选择加密整个分区。如果您为某分区启用了库存机管理加密，那么该分区中所有支持库存机管理加密的磁带机都将启用加密，写入该分区中支持介质的所有数据也将被加密。该分区中库存机管理加密不支持的磁带机都不会启用加密，写入无支持介质的数据也不会加密。

EKM 支持的磁带机中写入支持加密和能够加密介质的数据将被加密，除非之前是以非加密形式写入数据的。为了对数据进行加密，必须使用空白介质或者在磁带第一次写操作时 (BOT) 就已使用库存机管理加密功能写入数据。

按如下方式配置分区：

1. 从 “Web client”（Web 客户端），选择 “Setup”（**安装**）> “Encryption”（**加密**）> “Partition Configuration”（**分区配置**）。

   随即出现包含所有分区的列表，以及一个下拉列表，显示各分区的加密方法。

2. 如果您想更改某分区的加密方法，请确保该分区里的磁带机没有装入磁带。如果磁带机装有磁带，则不能更改加密方法。

3. 从下拉列表中为各个分区选择一种加密方法。（对于支持加密的磁带机，默认情况下为 Application Managed （应该程序管理）。）加密方法应用到分区中所有能够加密的磁带机和介质。

加密方法	说明
Library Managed（库存机管理）	**用于 EKM。**通过所连接的 Dell EKM 密匙服务器，为分配给该分区的所有能够加密的磁带和介质启用加密支持。
Application Managed（应用程序管理）	**不用于 EKM。**允许外部备份应用程序向分区中所有具备加密能力的磁带机和介质提供加密支持。库存机将不与该分区的 Dell EKM 服务器通信。 如果分区内有具备加密能力的磁带机，则默认设置为禁用。此选项应保持选定，*除非*您要使用 Dell EKM 管理加密。 **注意：**如果想要应用程序管理加密，必须专门配置应用程序以便管理加密。库存机不会参与执行这种类型的加密。
None （无）	禁用分区的加密。
Unsupported （不支持）	表示该分区中没有任何支持加密的磁带机。 如果显示 “Unsupported”（**不支持**），则设置将变为灰色且无法更改设置。

4. 如果您希望其他分区使用不同的 EKM 密匙服务器，请根据该步骤说明，填写库存机管理加密服务器的覆盖部分。覆盖部分中的设置将取代 “Setup”（**设置**）>“ Encryption”（**加密**)>“System Configuration”（**系统配置**）屏幕列出的默认设置。（但是，覆盖设置不会更改 “Setup”（**设置**）>“Encryption”（**加密**）>“System Configuration”（**系统配置**）屏幕中列出的设置。这些设置是任何没有使用覆盖的分区的默认配置设置。）只有在加密方法设置为 “Library Managed”（**库存机管理**）的分区上，覆盖才可用。

警告：如果您希望其他分区使用不同的 EKM 密匙服务器，请只填写覆盖部分。否则，将此部分保持不变，并允许 “Setup”（设置）>“Encryption”（加密）>“System Configuration”（系统配置）屏幕中的值填写这些字段。一旦您对覆盖部分做出任何更改，“Setup”（设置）>“Encryption”（加密）>“System Configuration”（系统配置）屏幕中的默认值就不会再自动填写这些字段。在更改覆盖之后，如果您要返回默认设置，则必须手动输入它们。

对于加密方法为 “Library Managed”（库存机管理）的每个分区，执行以下操作：

- 在 Primary Host （第一主机）文本框内键入第一 EKM 密匙服务器的 IP 地址 （ DNS 未启用）或主机名 （ DNS 启用）。

www.dell.com | support.dell.com

- 在 Port （端口）文本框内键入第一 EKM 密匙服务器的端口号。如果没有启用 SSL，则默认端口号是 3801。如果启用 SSL，则默认端口号是 443。
- 如果您使用的是第二 EKM 服务器，则在 Secondary Host （第二主机）和 Port （端口）文本框内键入第二 EKM 密匙服务器的地址 / 主机名和端口号。
- 如果您要对该分区和 EKM 服务器之间的通信启用安全套接字层 (SSL)，则选择 **SSL** 复选框。默认值为 "Disabled"（禁用）。如果您启用 SSL，则必须确保覆盖部分中的第一和第二 EKM 端口号与在 EKM 服务器上设置的 SSL 端口号匹配。默认 SSL 端口号是 443。

注意：无论是否启用 SSL，将密钥从 EKM 服务器发送到磁带机之前，始终都会将密钥加密。启用 SSL 可进一步增强安全性。

注意：EKM 服务器覆盖的限制：如果使用第一和第二服务器进行覆盖，则适用以下限制。（如果不使用第二服务器，则没有限制。）

限制：给定第一服务器和第二服务器必须 " 成对 "，且不能用于不同的组合。例如：
- 对于任何或所有分区，您已将 Server1 作为第一服务器并将 Server2 作为第二服务器。
- 如果在某个分区上 Server1 是第一服务器且 Server2 是第二服务器，那么在使用 Server1 的任何其他分区中，只能将 Server1 作为第一服务器，而且它必须与将 Server2 作为第二服务器 " 成对 "。在另一个分区中，您不能将 Server1 作为第一服务器而将 Server3 作为第二服务器。
- 不能将 Server1 既作为 PartitionA 的第一服务器，又作为 PartitionB 的第二服务器。
- 不能将 Server2 既作为 PartitionA 的第二服务器，又作为 PartitionB 的第一服务器。

如果您使用覆盖，则确保在指定的所有服务器上安装 Dell EKM。然后，在为 EKM 配置的每个分区的每个磁带机上运行 EKM 路径诊断，确保每个磁带机可与指定 EKM 服务器通信并从该服务器接收密钥。有关更多信息，请参阅 " 使用 EKM 路径诊断 "，位于第 58 页。

5 单击 "Apply"（**应用**）。

随即出现 "Progress Window"（进度窗口）。"Progress Window"（进度窗口）包含有关操作、已用时间和请求操作状态的信息。执行以下操作之一：

- 如果在 "Progress Window"（进度窗口）中出现 "**Success**"（**成功**），则表示已成功配置 EKM 系统设置。单击 "**Close**"（**关闭**）关闭 "Progress Window"（进度窗口）。
- 如果在 "Progress Window"（进度窗口）中出现 "**Failure**"（**失败**），则表示未成功配置 EKM 系统设置。按照 "Progress Window"（进度窗口）中列出的说明解决操作过程中出现的问题。

6 保存库存机配置 （要获得相关说明，请参阅 *Dell PowerVault ML6000 用户指南*）。

步骤 4：运行 EKM 路径诊断

运行 EKM 路径诊断以确保您的磁带机和密钥服务器已连接并正常工作。请参阅 " 使用 EKM 路径诊断 "，位于第 58 页。

备份 Keystore 数据

鉴于 Keystore 中密钥的关键性质，您需要在非加密设备中备份 Keystore，以便在需要之时能够恢复，并且能够读取使用与磁带机或库存机关联的加密密钥进行加密的磁带。

使用 EKM 路径诊断

EKM 路径诊断由一系列简短的测试组成，验证密匙服务器是否运行、已连接以及是否按要求提供密匙服务功能。

每次更改密匙服务器设置或库存机加密设置以及更换磁带机时，都要运行手动 EKM 路径诊断。建议您一一测试与密钥管理器服务器通信的磁带机。

诊断由以下测试组成：

注意：测试用的磁带机必须空载、准备就绪并联机，以运行任何测试。

- Ping — 验证库存机与密匙服务器之间的以太网通信链路。如果选定磁带机所在的分区使用 EKM 服务器覆盖，则会测试覆盖 IP 地址 （请参阅 “Setup”（设置） >“Encryption”（加密） > “Partition Configuration”（分区配置））。如果分区不使用覆盖，则会测试默认系统 IP 地址 （请参阅 “Setup”（设置） >“Encryption”（加密） >“System Configuration”（系统配置））。
- Drive — 验证磁带机在库存机中的路径 （从库存机到磁带机单端连接，以及从磁带机单端到磁带机连接）。磁带机必须空载、准备就绪并联机，以便运行该测试。如果测试失败，则不执行路径和配置测试。
- Path— 检验密匙服务器是否在运行 EKM 服务。如果磁带机测试失败，则无法运行该测试。
- Config — 检验密匙服务器是否能够支持加密密匙。如果磁带机测试失败，则无法运行该测试。

如果任何测试不通过，请尝试以下解决方法，并重新运行测试，保证测试通过：

- Ping Test Failure （Ping 测试不通过）— 检查密匙服务器主机是否在运行，可否通过与库存机相连接的网络访问。
- Drive Test Failure （磁带机测试不通过）— 查找任何磁带机 RAS 标签并按标签中的解决说明操作。
- Path Test Failure（路径测试不通过）— 检查密匙服务器是否确实在运行以及端口 /SSL 设置是否与库存机配置设置匹配。
- Config Test Failure （配置测试不通过） — 验证 EKM 服务器设置为接受您正测试的磁带机。

执行诊断的方法有两种：

- 自动 EKM 路径诊断依次测试各台相连的 EKM 服务器，库存机则选择各个测试所用的磁带机。如果所选的磁带机不可用 （磁带机必须空载、准备就绪并联机），那么库存机将尝试与服务器相连的其他磁带机，直至找到可用的磁带机。如果与特定密匙服务器相连的磁带机均不可用，则跳过该服务器，不执行测试。如果连续地服务器连续跳过 “X” 个测试间隔 （其中 “X” 可在 Web 客户端上配置），库存机将生成 RAS 票证。如果磁带机长时间保持加载状态，它可能不再接受测试。如果您想测试特定的磁带机，则应使用手动 EKM 路径诊断。特别是更换了磁带机后，请运行手动 EKM 路径诊断手动 EKM 路径诊断
- 自动 EKM 路径诊断

手动诊断与自动诊断有以下不同之处：

- 手动诊断会使受影响的分区脱机。自动诊断不会使分区脱机，但在磁带机接受测试时，诊断进度会放缓。
- 手动 EKM 路径诊断要求您选择一个磁带机用于测试。由于测试只验证选定的磁带机，如果您要测试每个磁带机的路径，则必须多次运行测试 （每个磁带机一次）。要测试所有服务器，您必须对启用库存机管理加密的各个分区进行一次诊断 （每对服务器与唯一的分区和磁带机相连）。此外，如果磁带机不可用 （磁带机必须空载、准备就绪并联机），则不执行磁带机、路径和配置测试。
- 自动 EKM 路径诊断依次测试各台相连的 EKM 服务器，库存机则选择各个测试所用的磁带机。如果所选的磁带机不可用 （磁带机必须空载、准备就绪并联机），那么库存机将尝试与服务器相连的其他磁带机，直至找到可用的磁带机。如果与特定密匙服务器相连的磁带机均不可用，则跳过该服务器，不执行测试。如果连续地服务器连续跳过 “X” 个测试间隔 （其中 “X” 可在 Web 客户端上配置），库存机将生成 RAS 票证。如果磁带机长时间保持加载状态，它可能不再接受测试。如果您想测试特定的磁带机，则应使用手动 EKM 路径诊断。特别是更换了磁带机后，请运行手动 EKM 路径诊断手动 EKM 路径诊断

1 采用以下两种方法之一访问 EKM 路径诊断屏幕：

- 进入 Library Diagnostics （库存机诊断）（选择 Tools （工具） > Diagnostics （诊断）），然后选择 EKM > EKM Path Diagnostics （EKM 路经诊断）。请注意，进入诊断将断开所有其他具有相同或较低权限的用户，并使分区脱机。当您退出 Diagnostics （诊断）时，分区将自动恢复联机。
- 选择 Setup （设置） > Encryption （加密） > System Configuration （系统配置）或 Setup （设置） > Encryption （加密） > Partition Configuration （分区配置），并单击 “ Click here to run EKM Path Diagnostics （单击此处运行 EKM 路经诊断） ”。请注意，执行此操作会使所选磁带机所在的分区脱机。当测试完成时，分区会自动恢复联机。

www.dell.com | support.dell.com

此时将显示为库存机管理的加密启用的所有磁带机列表，以及磁带机状态和每个磁带机所在的分区。

2 选择要执行诊断的磁带机，然后单击 "Apply" **（应用）**。磁带机必须空载、准备就绪并联机以运行测试。

此时将显示一个对话框，告诉您选定分区将变为脱机。

3 单击 "OK" **（确定）**以开始诊断。

随即出现 "Progress Window"（进度窗口）。"Progress Window"（进度窗口）包含有关操作、已用时间和请求操作状态的信息。

库存机执行诊断并在 "Progress Window"（进度窗口）的每项测试上报告通过 / 不通过结果。

注意：诊断测试可能需要几分钟才能完成。

4 执行以下操作之一：

- 如果 "Progress Window"（进度窗口）中出现 "Completed" **（已完成）**，表示已执行诊断 （这不表示诊断已通过，只是表示已执行诊断）。单击 "Close" **（关闭）**关闭 "Progress Window"（进度窗口）。
- 如果 "Progress Window"（进度窗口）中出现 "Failure" **（不通过）**，表示无法执行诊断。按照 "Progress Window"（进度窗口）中列出的说明解决操作过程中出现的问题。

自动 EKM 路径诊断

您可以让库存机按选定间隔自动执行 EKM 路径诊断。在每个间隔内，库存机会测试每个已配置的密匙服务器。如果出现问题，库存机会生成 RAS 票证。默认情况下，禁用此功能。默认测试间隔为四小时。建议您禁用自动 EKM 路径诊断，除非在您的站点加密失败通常是网络中断引起的。

警告：如果连续在可配置的间隔次数内因为磁带机不可用而跳过测试，运行 EKM 路径诊断会使 RAS 票证数量增多。为减少 RAS 票证的出现，您可以将生成 RAS 票证所需的连续测试间隔次数提高，或者将库存机设为在忽略测试的间隔内不再生成 RAS 票证。

有关已执行测试的列表，请参阅 " 使用 EKM 路径诊断 "，位于第 58 页。

要启用自动 EKM 路径诊断，请执行以下操作：

1 从 Web client （Web 客户端），选择 "Setup" **（设置）** > "Encryption" **（加密）** > "System Configuration" **（系统配置）**。

2 选中 Automatic EKM Path Diagnostics （自动 EKM 路径诊断）复选框。

3 从下拉列表选择一个测试间隔。

4 指定在库存机生成 RAS 票证之前所需的连续错误测试间隔的次数，该票证将通知您，在指定的间隔内无法执行测试。

查看磁带机加密设置

您可以通过以下方式查看加密设置：

- **系统信息报告 —** 要查看所有密匙服务器、分区和磁带机上的加密信息，请从 Web 客户端选择 "Reports" **（报告）** > "System Information" **（系统信息）**。有关详细信息，请参阅 《*Dell PowerVault ML6000 用户指南*》。
- **库存机配置报告 —** 要查看选定磁带机或磁带盒的加密状态，请从 Web 客户端选择 "Reports" **（报告）** > "Library Configuration"（库存机配置），然后单击磁带机或插槽。加密状态将显示在弹出状态窗口中。有关详细信息，请参阅 《*Dell PowerVault ML6000 用户指南*》。
- **分区加密 —** 从 Web 客户端，选择 "Setup" **（设置）** > "Encryption" **（加密）** > "Partition Configuration"（分区配置），以查看和更改分区的加密设置。有关详细信息，请参阅 " 步骤 3：配置分区加密 "，位于第 57 页。

請先閱讀 - 如何在 PowerVault™ ML6000 上設定 Dell Encryption Key Manager （Traditional Chinese）

關於警告

警告：警告表示如不按說明操作，可能會硬體損壞或資料丟失。

本文件目的

Dell Encryption Key Manager (EKM) 是一種中央密匙管理器應用程式，可管理作爲 IBM LTO-4 和 IBM LTO-5 基於磁帶機資料加密過程的一部分的加密密匙。媒體櫃管理加密是一種已獲授權的可選功能，該功能必須從 PowerVault ML6000 媒體櫃啓用，以便使用 LTO-4/LTO-5 磁帶機加密功能開始對資料進行加密。

Dell EKM 是 IBM Java 軟體程式，能協助啓用加密功能的磁帶機來產生、防護、儲存和維護密鑰（用來爲正在寫入磁帶媒體的資訊加密，及爲正在讀取磁帶媒體的資料解密）。由於策略控制和密匙經過媒體櫃，因此應用程式可以「看到」加密。

有關安裝和設定 EKM 伺服器和 Dell EKM 最佳做法的更多資訊，請參閱 *《Dell PowerVault Encryption Key Manager 使用者指南》*和 *《Dell Encryption Key Manager 和媒體櫃管理加密最佳做法與常見問題解答一覽表》*。

註：為了讓 Dell EKM 能正確工作，您必須將媒體櫃和磁帶機韌體升級至最新釋出的版本。 以下網址提供最新的固件和安裝說明：http://support.dell.com。

支持的磁帶機和介質

PowerVault ML6000 的媒體櫃管理加密功能僅在使用 IBM LTO-4 和 LTO-5 光纖通道和 SAS 磁帶機的 LTO-4 和 LTO-5 資料磁帶上支援加密。ML6000 媒體櫃管理加密在其他類型磁帶機或製造商品牌產品時不支援加密，即使將它們分配到一個爲加密而選擇的分割也不支持加密。其他介質類型（例如，LTO-3）可以被啓用媒體櫃管理加密功能的磁帶機讀取，但不能進行加密。

在伺服器上安裝 Dell EKM

您必須提供一個或多個用來安裝 Dell EKM 的伺服器。您購買媒體櫃管理加密時，就可獲得一張 CD，裏面包含用於在伺服器上安裝的軟體，以及安裝說明和使用者指南。您必須先設定 EKM 伺服器併安裝授權碼，才能在媒體櫃上設定 EKM。

註：由於 Dell PowerVault ML6000 媒體櫃在啟用加密的磁帶機中讀取或寫入資料時需要與 EKM 伺服器即時通信，強烈建議您同時使用第一和第二 EKM 伺服器。以上述方式，若主要伺服器在媒體櫃需要加密資訊時無法使用，次要伺服器便可以接著處理其要求。Dell PowerVault ML6000 媒體櫃允許您出於故障轉移 / 冗餘的目的使用最多兩個伺服器。

設定媒體櫃上的加密功能

步驟 1：安裝授權碼

註：確認您的媒體櫃和磁帶機韌體皆已更新至最新的版本。最新的韌體和安裝說明能在 www.support.dell.com 中找到。

1 若要取得授權碼以進行加密，請依照您收到的「*授權認證碼*」上的說明來操作。

2 執行以下之一的操作：
- 從操作器面板中，選擇 Setup（**設定**）> Licenses（**授權**）。
- 從網頁用戶端，選擇 Setup（**設定**）> License（**授權**）。

3 輸入新的授權碼。

4 按 Apply（**套用**）一下。

會出現進度視窗顯示已經過的時間。完成時，會出現綠色的 Success（**成功**）訊息，且狀態會變更爲「操作成功」。現在加密會在螢幕上列爲功能。（如果出現 Failure（**失敗**）訊息，可能是您輸入了不正確的授權碼。）

5 按 Close（**關閉**）一下。

步驟 2：設定加密設置和密鑰伺服器位址

1 從媒體櫃裏中的所有可加密磁帶機上取出磁帶卡匣。

2 從網頁用戶端，選擇 Setup（**設定**）> Encryption（**加密**）> System Configuration（**系統設定**）。

3 Automatic EKM Path Diagnostics（**自動 EKM 路徑診斷**）：啓用或禁用這個功能，並根據需要設置測試時間間隔。您也可以具體指定生成 RAS 票證所需的連續忽略測試時間間隔次數。請參閱自動 EKM 路徑診斷 於第 66 頁，以得到更多詳細資料。

4 **安全套接字層** (SSL)：要啓用 SSL 以便媒體櫃和 EKM 密匙伺服器進行通信，請選擇「SSL Connection」（**SSL 連接**）核取方塊。預設值是停用。如果您啓用了 SSL，您必須確保**第一**和**第二密匙伺服器埠號**（見下文）與 EKM 密匙伺服器上的 SSL 通訊埠碼匹配。預設的 SSL 通訊埠碼爲 443。

註：無論是否啟用 SSL，密匙始終在從 EKM 密匙伺服器發送到磁帶機之前進行加密。啟用 SSL 會使安全性更高。

5 在 Primary Key Server IP Address or Host（**第一密匙伺服器 IP 位址或主機**）文本框中，輸入以下項之一：
- 第一密匙伺服器的 IP 位址（ DNS 未用），或
- 第一密匙伺服器的主機名（ DNS 啓用）。

6 在 Primary Key Server Port Number（**第一密匙伺服器通訊埠碼**）文本框中輸入第一密匙伺服器的通訊埠碼。只要不啓用 SSL，預設的通訊埠碼就爲 3801。如果啓用了 SSL，則預設的通訊埠碼爲 443。

註：如果您更改媒體櫃的通訊埠碼設置，您也必須相應地更改密匙伺服器的通訊埠碼，否則 EKM 將無法正常工作。

7 如果您出於故障轉移的目的使用第二密匙伺服器，則在 Secondary Key Server IP Address or Host（**第二密匙伺服器 IP 位址或主機**）文本框中輸入第二密匙伺服器的 IP 位址或主機名。

註：如果您不打算使用第二密匙伺服器，您可在 **Secondary Key Server IP Address or Host（第二密匙伺服器 IP 位址或主機名）**文本框中輸入零 IP 位址，即 0.0.0.0，或者留空不填。

8 如果您設定了第二密匙伺服器（前一步驟），請在 Secondary Key Server Port Number（**第二密匙伺服器通訊埠碼**）文本框中輸入第二密匙伺服器的通訊埠碼。只要不啓用 SSL，預設的通訊埠碼就爲 3801。如果啓用了 SSL，則預設的通訊埠碼爲 443。

註：如果您要使用第二密匙伺服器，則第一和第二密匙伺服器的通訊埠碼必須設為同一值。如果不設為同一值，將不會執行同步和故障轉移。

9 按 Apply（**套用**）一下。

會開啓「進度視窗」。「進度視窗」包含動作的資訊、已經過時間，以及操作的狀態。執行以下之一的操作：
- 如果「進度視窗」中有顯示 Success（**成功**），則 EKM 系統已成功完成設定。按 Close（**關閉**）一下來關閉「進度視窗」。
- 如果「進度視窗」中有顯示 Failure（**失敗**），則 EKM 系統設定尚未完成。依照「進度視窗」中所列出的指示來解決任何操作中發生的問題。

註：如果您打算對不同的分割使用不同的 EKM 密匙伺服器，您也必須填寫 Setup（**設置**）> Encryption（**加密**）> Partition Encryption（**分割加密**）螢幕上的覆蓋部分。請參閱步驟 3：設定分割磁區加密。

步驟 3：設定分割磁區加密

僅能按分割對 Dell PowerVault ML6000 磁帶媒體櫃進行加密。您無法選擇個別的磁帶機來加密，必須選擇一整個磁碟分割區來加密。如果您爲某分割啓用了媒體櫃管理加密，那麼該分割中所有支援函式媒體櫃管理加密的磁帶機都將啓用加密，寫入該分割中支援介質的所有資料也將被加密。該分割中媒體櫃管理加密不支援的磁帶機都不會啓用加密，寫入無支援介質的資料也不會加密。

EKM 支援的磁帶機中寫入支援加密和能夠加密介質的資料將被加密，*除非*之前是以非加密形式寫入資料的。爲了對資料進行加密，必須使用空白介質或者在磁帶第一次寫操作時 (BOT) 就已使用媒體櫃管理加密功能寫入資料。

如以下方式來設定分割區：

1 從網頁用戶端，選擇 **Setup（設定）> Encryption（加密）> Partition Configuration（分割區設定）**。

隨即出現包含所有分割的列表 ，以及一個下拉清單，顯示各分割的加密方法。

2 如果您想更改某分割的加密方法，請確保該分割裏的磁帶機沒有裝入磁帶。如果磁帶機裝有磁帶，則不能更改加密方法。

3 從下拉清單中爲各個分割選擇一種加密方法。（對於支援加密的磁帶機，預設情況下爲 **Application Managed（應該程式管理）**。）加密方法應用到分割中所有能夠加密的磁帶機和介質。

加密方法	說明
Library Managed（媒體櫃管理式）	**與 EKM 配合使用。**透過所連接的 Dell EKM 密匙伺服器，爲分配給該分割的所有能夠加密的磁帶和介質啓用加密支援。
Application Managed（應用程式管理式）	**不用於 EKM。**允許外部備份應用程式向分割中所有具備加密能力的磁帶機和介質提供加密支援。此媒體櫃將「無法」和該分割區中的 Dell EKM 伺服器進行通訊。 如果您在分割區中有具加密功能的磁帶機，這將會是預先設定。應保持選擇此選項，*除非*您希望 Dell EKM 來管理加密。 **註：如果您想要讓應用程式管理加密，必須特別設定該應用程式來執行。媒體櫃將不會參與此類型的加密執行作業。**
無	停用分割區加密。
Unsupported（不支援的）	表示該分割區中沒有支援加密功能的磁帶機。 如果畫面中顯示 **Unsupported（不支援的）**，分割區將會顯示爲灰色且您無法變更設定。

4 如果您希望其他分割使用不同的 EKM 密匙伺服器，請根據該步驟說明，填寫媒體櫃管理加密伺服器的覆蓋部分。覆蓋部分中的設置將取代 **Setup（設置）> Encryption（加密）> System Configuration（系統設定）**螢幕列出的預設設置。（但是，覆寫設定不會變更 **Setup [設定] > Encryption [加密] > System Configuration [系統設定]** 螢幕中列出的設定。這些設定爲所有不使用覆寫設定的分割區的預設設定。）僅使用 **Library Managed（媒體櫃管理式）**設定作爲加密方法的分割區可以使用覆寫設定。

△ **警告：如果您希望其他分割使用不同的 EKM 密匙伺服器，請只填寫覆蓋部分。否則，請不要管此區段，允許 Setup （設定）> Encryption （加密）> System Configuration （系統設定）螢幕中的值填寫這些欄位。一旦您對覆寫區段做了任何變更，Setup （設定）> Encryption （加密）> System Configuration （系統設定）螢幕中的預設值將不再自動填寫這些欄位。如果希望在變更了覆寫設定後回到預設設定，則您必須手動輸入它們。**

對於每個使用「媒體櫃管理式」作爲加密方法的分割區，請執行以下操作：

- 在 **Primary Host（第一主機）**文本框內鍵入第一 EKM 密匙伺服器的 IP 位址 （ DNS 未啓用）或主機名 （ DNS 啓用）。
- 在 **Port（埠）**文本框內鍵入第一 EKM 密匙伺服器的通訊埠碼。只要不啓用 SSL，預設的通訊埠碼就爲 3801。如果啓用了 SSL，則預設的通訊埠碼爲 443。

www.dell.com | support.dell.com

- 如果您使用的是第二 EKM 伺服器，則在 **Secondary Host（第二主機）**和 **Port （埠）**文本框內鍵入第二 EKM 密匙伺服器的位址 / 主機名和通訊埠碼。
- 如果您要爲分割區與 EKM 伺服器之間的通訊啓用 Secure Sockets Layer （安全通訊端階層）(SSL)，則請選擇 **SSL** 核取方塊。預設值是停用。 如果您啓用了 SSL ，您必須確保第一和第二密匙伺服器通訊埠碼（見下文）與 EKM 密匙伺服器上的 SSL 通訊埠碼匹配。預設的 SSL 通訊埠碼爲 443。

註：不管是否啟用 SSL，密鑰在從 EKM 伺服器傳送到磁帶機之前，始終是加密的。啟用 SSL 會使安全性更高。

註：EKM 伺服器覆蓋的限制：如果使用第一和第二伺服器進行覆蓋，則適用以下限制。 （如果不使用第二伺服器，則沒有限制。）

限制：給定第一伺服器和第二伺服器必須「成對」，且不能用於不同的組合。例如：
- 對於任何或所有分割，您已將 Server1 作為第一伺服器並將 Server2 作為第二伺服器。
- 如果在某個分割上 Server1 是第一伺服器且 Server2 是第二伺服器，那麼在使用 Server1 的任何其他分割中，只能將 Server1 作為第一伺服器，而且它必須與將 Server2 作為第二伺服器「成對」。在另一個分割中，您不能將 Server1 作為第一伺服器而將 Server3 作為第二伺服器。
- 能將 Server1 既作為 PartitionA 的第一伺服器，又作為 PartitionB 的第二伺服器。
- 不能將 Server2 既作為 PartitionA 的第二伺服器，又作為 PartitionB 的第一伺服器。

如果使用覆寫設定，請確定在您指定的所有伺服器上安裝 Dell EKM。然後，在爲 EKM 設定的每個分割的每個磁帶機上運行 EKM 路徑診斷，確保每個磁帶機可與指定 EKM 伺服器通信並從該伺服器接收密鑰。請參閱使用 EKM 路徑診斷 於第 64 頁，以得到更多詳細資料。

5 按 Apply **（套用）**一下。

會出現「進度視窗」。「進度視窗」包含動作的資訊、經過時間，以及所要求操作的狀態。執行以下之一的操作：

- 如果「進度視窗」中有顯示 **Success （成功）**，則 EKM 系統已成功完成設定。按 **Close （關閉）**一下來關閉「進度視窗」。
- 如果「進度視窗」中有顯示 **Failure （失敗）**，則 EKM 系統設定尚未完成。依照「進度視窗」中所列出的指示來解決任何操作中發生的問題。

6 儲存媒體櫃設定 （如需說明，請參閱 *《Dell PowerVault ML6000 使用指南》*。）

步驟 4：運行 EKM 路徑診斷

運行 EKM 路徑診斷以確保您的磁帶機和密鑰伺服器已連接並正常工作。請參閱使用 EKM 路徑診斷 於第 64 頁。

備份 Keystore 資料

鑒於 Keystore 中密鑰的關鍵性質，您需要在非加密設備中備份 Keystore，以便在需要之時能夠恢復，並且能夠讀取使用與磁帶機或媒體櫃關聯的加密密鑰進行加密的磁帶。

使用 EKM 路徑診斷

EKM 路徑診斷由一系列簡短的測試組成，驗證密匙伺服器是否運行、已連接以及是否按要求提供密匙服務功能。

每次更改密匙伺服器設置或媒體櫃加密設置以及更換磁帶機時，都要運行手動 EKM 路徑診斷。建議您一一測試與密鑰管理器伺服器通信的磁帶機。

診斷由下列測試組成：

註： 測試用的磁帶機必須空載、準備就緒並聯機，以運行任何測試。

- Ping — 驗證媒體櫃與密匙伺服器之間的乙太網通信鏈路。如果選擇的磁帶機所駐留的分割區使用了 EKM 伺服器覆寫設定，則將測試覆寫 IP 位址（請參閱 Setup [**設定**] > Encryption [**加密**] > Partition Configuration [**分割區設定**]）。如果此分割區不使用覆寫設定，則將測試預設的系統 IP 位址（請參閱 Setup [**設定**] > Encryption [**加密**] > Partition Configuration [**分割區設定**]）。
- Drive — 驗證磁帶機在媒體櫃中的路徑（從媒體櫃到磁帶機單端連接，以及從磁帶機單端到磁帶機連接）。磁帶機必須空載、準備就緒並聯機，以便運行該測試。如果測試失敗，則不執行路徑和設定測試。
- Path — 檢驗密匙伺服器是否在運行 EKM 服務。如果磁帶機測試失敗，則無法運行該測試。
- Config — 檢驗密匙伺服器是否能夠支持加密密匙。如果磁帶機測試失敗，則無法運行該測試。

如果某個測試失敗，請嘗試以下解決方法，然後重新執行該測試，確保其通過：

- Ping Test Failure Ping（**測試不通過**） — 檢查密匙伺服器主機是否在運行，可否透過與媒體櫃相連接的網路存取。
- Drive Test Failure（**磁帶機測試失敗** ） — 尋找所有 RAS 票證，並根據票證中的解決方法說明進行操作。
- Path Test Failure（**路徑測試不通過** ） — 檢查密匙伺服器是否確實在運行以及埠 /SSL 設置是否與媒體櫃設定設置匹配。
- Config Test Failure（**設定測試失敗** ） — 驗證 EKM 伺服器是否設定爲接受您所測試的磁帶機。

執行診斷的方法有兩種：

- 手動 EKM 路徑診斷
- 自動 EKM 路徑診斷

手動診斷與自動診斷有以下不同之處：

- 手動診斷會使受影響的分割脫機。自動診斷不會使分割脫機，但在磁帶機接受測試時，診斷進度會放緩。
- 手動 EKM 路徑診斷要求您選擇一個磁帶機用於測試。由於測試只驗證選定的磁帶機，如果您要測試每個磁帶機的路徑，則必須多次運行測試（每個磁帶機一次）。要測試所有伺服器，您必須對啓用媒體櫃管理加密的各個分割進行一次診斷（每對伺服器與唯一的分割和磁帶機相連）。此外，如果磁帶機不可用（磁帶機必須空載、準備就緒並聯機），則不執行磁帶機、路徑和設定測試。
- 自動 EKM 路徑診斷依次測試各台相連的 EKM 伺服器，媒體櫃則選擇各個測試所用的磁帶機。如果所選的磁帶機不可用（磁帶機必須空載、準備就緒並聯機），那麼媒體櫃將嘗試與伺服器相連的其他磁帶機，直至找到可用的磁帶機。如果與特定密匙伺服器相連的磁帶機均不可用，則跳過該伺服器，不執行測試。如果連續地伺服器連續跳過「X」個測試間隔（其中「X」可在 網頁用戶端上設定），媒體櫃將生成 RAS 票證。如果磁帶機長時間保持載入狀態，它可能不再接受測試。**如果您想測試特定的磁帶機，則應使用手動 EKM 路徑診斷。特別是更換了磁帶機後，請運行手動 EKM 路徑診斷。**

手動 EKM 路徑診斷

1. 採用以下兩種方法之一存取 EKM 路徑診斷螢幕：
   - 進入 Library Diagnostics（媒體櫃診斷）（選擇 **Tools（工具）> Diagnostics（診斷）**），然後選擇 **EKM > EKM Path Diagnostics（EKM 路經診斷）**。請注意，進入診斷將斷開所有其他具有相同或較低許可權的用戶，並使分割脫機。當您退出 Diagnostics（診斷）時，分割將自動恢復聯機。
   - 選擇 **Setup（設置）> Encryption（加密）> System Configuration（系統設定）> Setup（設置）> Encryption（加密）> Partition Configuration（分割設定）**，並按一下「 Click here to run EKM Path Diagnostics」（按一下此處運行 EKM 路經診斷）。請注意，執行此操作會使所選磁帶機所在的分割脫機。測試結束後，此分割區將自動返回連線狀態。

www.dell.com | support.dell.com

將顯示爲媒體櫃管理式加密啓用的所有磁帶機的清單，以及磁帶機狀態和每個磁帶機所駐留的分割區。

2 請選擇要對其執行診斷的磁帶機，並按 Apply（**套用**）。磁帶機必須空載、準備就緒並聯機以運行測試。

出現的對話方塊會提示您選擇的分區將離線。

3 請按 OK（**確定**）來啓動診斷。

會出現「進度視窗」。「進度視窗」包含動作的資訊、經過時間，以及所要求操作的狀態。

媒體櫃將執行診斷，並在「進度視窗」中報告每項測試的通過 / 失敗結果。

註：診斷測試可能需要數分鐘時間來完成。

4 執行以下之一的操作：

- 如果「進度視窗」中顯示 Completed（**已完成**），則表示已執行診斷（這並不表示診斷通過，只表示已執行診斷）。按 Close（**關閉**）一下來關閉「進度視窗」。
- 如果「進度視窗」中顯示 Failure（**失敗**），則無法執行診斷。依照「進度視窗」中所列出的指示來解決任何操作中發生的問題。

自動 EKM 路徑診斷

您可以讓媒體櫃按選定間隔自動執行 EKM 路徑診斷。在每個間隔內，媒體櫃會測試每個已設定的密匙伺服器。如果出現問題，媒體櫃會生成 RAS 票證。 預設禁用此功能。預設測試間隔爲四小時。建議您禁用自動 EKM 路徑診斷，除非在您的站點加密失敗通常是網路中斷引起的。

警告：如果連續在可設定的間隔次數內因為磁帶機不可用而跳過測試，運行 EKM 路徑診斷會使 RAS 票證數量增多。為減少 RAS 票證的出現，您可以將生成 RAS 票證所需的連續測試間隔次數提高，或者將媒體櫃設為在忽略測試的間隔內不再生成 RAS 票證。

有關已執行測試的列表，請參閱 使用 EKM 路徑診斷 於第 64 頁。

要啓用自動 EKM 路徑診斷，請執行以下操作：

1 從網頁用戶端，選擇 Setup（**設定**）> Encryption（**加密**）> System Configuration（**系統設定**）。

2 選中 Automatic EKM Path Diagnostics（**自動 EKM 路徑診斷**）核取方塊。

3 從下拉清單選擇一個測試間隔。

4 指定在媒體櫃生成 RAS 票證之前所需的連續錯誤測試間隔的次數，該票證將通知您，在指定的間隔內無法執行測試。

檢視磁帶機加密設置

您可以透過以下方式檢視加密設置：

- System Information Report（**系統資訊報告** ）— 要檢視所有密匙伺服器、分割和磁帶機上的加密資訊，請從網頁用戶端選擇 Reports（**報告**）> System Information（**系統資訊**）。*有關詳細資訊，請參閱《Dell PowerVault ML6000 使用者指南》。*
- Library Configuration Report（**媒體櫃設定報告** ）— 要檢視選定磁帶機或磁帶卡匣的加密狀態，請從網頁用戶端選擇 Reports（**報告**）> Library Configuration（**媒體櫃設定**），然後按一下磁帶機或插槽。加密狀態將會顯示於快顯狀態視窗中。有關詳細資訊，請參閱 *《Dell PowerVault ML6000 使用者指南》。*
- Partition Encryption（**分割加密**）— 從網頁用戶端，選擇 Setup（**設置**）> Encryption（**加密**）> Partition Configuration（**分割設定**），以檢視和更改分割的加密設置。有關詳細資訊，請參閱 步驟 3：設定分割磁區加密 於第 63 頁 。